

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

IN RE

No. C-12-md-2330 EMC

CARRIER IQ, INC.,
CONSUMER PRIVACY LITIGATION.

**ORDER GRANTING IN PART AND
DENYING IN PART DEFENDANTS'
MOTION TO DISMISS SECOND
CONSOLIDATED AMENDED
COMPLAINT**

(Docket No. 304)

I. INTRODUCTION

Plaintiffs in this multidistrict litigation – eighteen (18) individuals from thirteen different states – have filed a second consolidated amended complaint (“SCAC” or “Complaint”) against Defendant Carrier IQ, Inc. and a number of manufacturers of mobile devices. The Complaint alleges that Defendants have violated the Federal Wiretap Act as well as a number of state’s privacy and consumer protection statutes through the creation and use of Carrier IQ’s software on Plaintiffs’ mobile devices. Plaintiffs allege that Carrier IQ designed, and the Device Manufacturers Defendants embedded, the Carrier IQ Software on their mobile devices and, once embedded, this software surreptitiously intercepted personal data and communications and transmitted this data to Carrier IQ and its customers. Pending before the Court is Defendants’¹ joint motion to dismiss the SCAC in its entirety. For the reasons that follow, the Court **GRANTS** in part and **DENIES** in part Defendants’ joint motion, and will afford Plaintiffs leave to file a third consolidated amended complaint.

¹ Originally, all the Defendants moved to dismiss the SCAC. After the hearing on the motions to dismiss, Carrier IQ, Inc. reached a settlement with Plaintiffs and subsequently withdrew their motion to dismiss. *See* Docket Nos. 322, 334. The remaining Defendants are referred to either as “Defendants” or as “Device Manufacturers” throughout this order.

II. FACTUAL & PROCEDURAL BACKGROUND

A. Plaintiffs

There are 18 plaintiffs in this action, from 13 different states. Below is a chart that identifies the Plaintiff, the state in which each resided during the relevant period, and which mobile device each Plaintiff had with the Carrier IQ Software installed:

Plaintiff	State	Device
Patrick Kenny	Arizona	Samsung Galaxy S 4G HTC Touch
Daniel Pipkin	California	Samsung Galaxy SII 4G LTE
Jennifer Patrick	California	Motorola Bravo
Dao Phong	California	HTC EVO
Ryan McKeen	Connecticut	Samsung Epic Touch 4G
Leron Levy	Florida	Samsung Moment
Matthew Hiles	Iowa	LG Marquee
Luke Szulczewski	Illinois	HTC EVO 4G
Michael Allan	Kentucky	HTC EVO 4G
Gary Cribbs	Maryland	Samsung Galaxy S2
Shawn Grisham	Mississippi	Samsung Epic 4G
Bobby Cline	Michigan ²	LG LS670 Optimus S
Mark Laning	Texas	Pantech P5000
Clarissa Portales	Texas	HTC EVO
Douglas White	Texas	Huawei Ascend II m865
Eric Thomas	Texas	Samsung Replenish
Brian Sandstrom	Washington ³	HTC EVO
Colleen Fischer	Wisconsin	LG LS670 Optimus S

² Mr. Cline resides in New Hampshire, but the SCAC alleges that “at pertinent times to this matter, he resided in Oakland County, Michigan.” SCAC ¶ 19. Accordingly, for purposes of this order, Mr. Cline will be treated as a resident of Michigan.

³ Mr. Sandstrom is a resident of California, but the SCAC alleges that “at pertinent times to this matter, he resided in Seattle, Washington.” SCAC ¶ 24.

In describing each Plaintiff, the SCAC provides that “[u]pon information and belief, [the Plaintiff’s] mobile device came with the Carrier IQ Software and implementing or porting software pre-installed. In addition to using his devices to make phone calls, [the Plaintiff] has used it for web browsing and text messaging, including accessing, inputting, and transmitting personal, private, confidential, and sensitive information. [The Plaintiff] would not have purchased his mobile device had he known that the Carrier IQ Software and related implementing or porting software was installed and operating on his device, and taxing his device’s battery, processor, and memory, as alleged herein.” *See* SCAC ¶¶ 8-25.

B. Defendants

The remaining defendants in this action are a number of mobile device manufacturers. Plaintiffs allege that Carrier IQ is the “designer, author, programmer, and vendor” of the IQ Agent software and provided the mobile device manufacturers the “guide or template” needed for the “related implementing or porting software known as the CIQ Interface.” *Id.* ¶ 26. The IQ Agent and CIQ Interface software forms the basis of Plaintiffs’ claims, as described *infra*.

The remaining Defendants are: (1) HTC America, Inc. and HTC Corporation (collectively “HTC”); (2) Huawei Device USA, Inc. (“Huawei”), (3) LG Electronics MobileComm U.S.A., Inc. and LG Electronics, Inc. (collectively “LG”); (4) Motorola Mobility LLC (“Motorola”); (5) Pantech Wireless, Inc. (“Pantech”); (6) Samsung Telecommunications America, Inc. and Samsung Electronics Co., Ltd. (collectively “Samsung”). Each Defendant is alleged to have installed the Carrier IQ Software and CIQ Interface software on at least some of their mobile device models.

C. Asserted Causes of Action

The SCAC alleges five causes of action:

- **Count 1: Violation of the Federal Wiretap Act (18 U.S.C. § 2551)**
- **Count 2: Violation of State Privacy Laws:** Plaintiffs assert their claims on behalf of all residents of the United States under Cal. Penal Code § 502 and on behalf of citizens of the following 35 states under those states’ respective privacy laws: Arizona, California, Connecticut, Delaware, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.

- **Count 3: Violation of State Consumer Protection Acts:** Asserted on behalf of residents of the following 21 states under those states' respective consumer protection statutes: Arkansas, California, Connecticut, Delaware, Florida, Hawaii, Kansas, Maryland, Michigan, Missouri, Nevada, New Hampshire, New Jersey, Oklahoma, Rhode Island, South Carolina, South Dakota, Texas, Vermont, Washington, and West Virginia.
- **Count 4: Violation of the Magnuson-Moss Warranty Act (15 U.S.C. § 2301-2312):** Asserted on behalf of the residents of the following 34 states (and the District of Columbia): Alaska, Arkansas, California, Colorado, Delaware, District of Columbia, Hawaii, Indiana, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Dakota, Oklahoma, Pennsylvania, Rhode Island, South Carolina, South Dakota, Texas, Utah, Virginia, Washington, West Virginia, and Wyoming.
- **Count 5: Violation of the Implied Warranty of Merchantability:** asserted on behalf of residents of the states enumerated under Count 4.

D. Carrier IQ Software Background

Carrier IQ “designed, authored, programmed, and caused the installation and activation of the Carrier IQ Software, including the so-called IQ Agent, on the devices at issue in this case.” *Id.* ¶ 62. It also “designed, authored, and provided guides to the Device Manufacturers for designing, authoring, programming, installing, and activating the CIQ Interface in deployments” through the “embedded” method of installation. *Id.*

Carrier IQ represents that its software is a “network diagnostics tool” for cell phone service providers. *Id.* ¶ 40. It is alleged that in reality, the software collects, and transfers, sensitive personal data off of a user’s mobile device. *See id.* ¶¶ 1-2. Specifically, the CIQ Interface software is alleged to be a “wrapping or porting layer of code designed to see recognize and intercept a host of data and content, including SMS text message content and URLs containing search terms, user names, and passwords . . . and to send that material down to the IQ Agent further processing and possible transmittals.” *Id.* ¶ 63. The SCAC alleges that the Device Manufacturers “design and program” the CIQ Interface (with Carrier IQ’s aid) and then install the CIQ Interface and IQ Agent software on their mobile devices. *Id.* Once installed, the software “operates in the background,” such that the typical user has no idea that it is running and cannot turn it off. *Id.* ¶ 64.⁴ Users are

⁴ It is alleged that even users with advanced technical skills can only remove the Carrier IQ Software by “rooting” their devices and voiding the warranties of their devices. *Id.* ¶ 64.

1 never given the choice of opting into or out of the Carrier IQ Software’s functionality. *Id.* Because
2 it is always running, the Plaintiffs allege that it “taxes the device’s battery power, processor
3 functions, and system memory.” *Id.*

4 Plaintiffs allege that the data intercepted by the Carrier IQ Software includes the following:
5 (1) URLs (including those which contain query strings with embedded information such as search
6 terms, user names, passwords, and GPS-based geo-location information); (2) GPS-location
7 information; (3) SMS text messages; (4) telephone numbers dialed and received; (5) the user’s
8 keypad presses/keystrokes; and (6) application purchases and uses. *Id.* ¶ 65. This information is
9 intercepted as part of the Carrier IQ Software’s “calls” on the device operating system for “metrics.”
10 *Id.* It then stores the information in the mobile device’s RAM memory on a rolling basis. *Id.*

11 The Carrier IQ Software also has a feature referred to as “Profiles.” Via Profiles, Carrier IQ
12 customers (who are typically wireless carriers, but can also include device manufacturers) will
13 specify which data they want from the above described “metrics.” *Id.* ¶ 68. At designated times (or
14 as requested), the Profile-specified data would then be transmitted from the mobile device to the
15 requesting customer (the wireless carriers or device manufacturers). *Id.*

16 The SCAC quotes from a number of letters which the various Device Manufacturers sent to
17 Senator Al Franken in response to his inquiries regarding the Carrier IQ Software. These letters
18 provide a glimpse into the potential scope of the Carrier IQ Software deployment. AT&T stated that
19 Carrier IQ’s Software was installed on approximately “900,000 devices, with about 575,000 of those
20 collecting and reporting wireless and service performance information to AT&T.” *Id.* ¶ 53. Sprint
21 indicated that there were “26 million active Sprint devices that have Carrier IQ Software Installed”
22 and stated that Sprint queried information from a fraction of those (c. 1.3 million) at any given time
23 for diagnostic needs and that a 30,000 device subset of this 1.3 million were used for “research
24 specific problems.” *Id.* ¶ 54. T-Mobile stated that there were “approximately 450,000 T-Mobile
25 customers [that] use devices that contain Carrier IQ’s diagnostic software.” *Id.* ¶ 56.

26 The SCAC recounts two ways where deployment of the Carrier IQ Software has resulted in
27 “grave breaches of privacy.” *Id.* ¶ 69. First, due to a “programming error,” the SCAC alleges that
28 AT&T has admitted that the “Carrier IQ Software transmitted text message content to it.” *Id.*

Plaintiffs use this as evidence that the Carrier IQ Software does, in fact, intercept and capture text message content. *Id.* Second, Plaintiffs state that “with some deployments, including those on HTC mobile devices and possibly on certain other devices,” the data and content intercepted by the Carrier IQ Software was sent in unencrypted, human-readable form into the system logs of the affected devices. *Id.* ¶ 71. Accordingly, this information was vulnerable to anyone with access to the system logs, including to individuals with malicious intent. *Id.* ¶ 72. Further, because this information was contained in system logs, the private information improperly intercepted and stored was transmitted to Google (who is the author of the Android Operating System) as part of crash reports. *Id.* ¶ 73. Similarly, HTC has acknowledged that they have also received this private information through its “Tell HTC” tool which “draws on content stored in the device logs.” *Id.* Accordingly, Plaintiffs contend that this information “may have gone to application developers who draw on device logs as a means of diagnosing application crashes (or for other purposes), including via widely available software tools.” *Id.*

Plaintiffs allege that the Carrier IQ Software continues to operate even if the consumer is using the device solely on a Wi-Fi network (as opposed to a cellular network). *Id.* ¶ 74.

E. FTC Investigation of and Action Against HTC Re: Carrier IQ Software

Since the filing of the First Consolidated Amended Complaint in this action, the FTC commenced an investigation into HTC regarding the Carrier IQ Software and a “related privacy and security flaw” in HTC mobile devices. *Id.* ¶ 75. This investigation culminated in a Consent Order agreement in February 2013. *Id.* ¶ 76.

The FTC found that HTC had “failed to take reasonable steps to secure the software it developed for its smartphones and tablet computers, introducing security flaws that placed sensitive information about millions of consumers at risk.” *Id.* One of the failures cited, was HTC’s failure to use “documented secure communications mechanisms in implementing logging applications,” thus placing sensitive information at risk. *Id.* ¶ 77. Because of HTC’s failure to implement security measures, “any third-party application that could connect to the internet could communicate with the logging applications on HTC devices and access a variety of sensitive information.” *Id.* One of the “logging” applications noted by the FTC was the Carrier IQ Software. Relevant to this case, the

Consent Order noted: The information collected by the Carrier IQ software was supposed to have been accessible only by network operators, but because HTC used an insecure communications mechanism, any third-party application on the user's device that could connect to the internet could exploit the vulnerability to communicate with the CIQ Interface." *Id.* This permitted interception of "the sensitive information being collected by the Carrier IQ software" and potentially allowed individuals to perform "malicious actions" such as "sending text messages without permission." *Id.*

The FTC Consent Order explained how this security flaw occurred. During the development of its CIQ Interface, HTC activated "debug code" in the operating system to test whether the CIQ Interface was operating properly. "The debug code accomplished this by writing the information to a particular device log known as the Android system log, which could then be reviewed. However, HTC failed to deactivate the debug code before its devices shipped for sale to consumers." *Id.* Thus, "all information that the CIQ Interface sent to the Carrier IQ software . . . was also written to the Android system log on the device." *Id.* Once in the system log, the sensitive information was then "[a]ccessible to any third-party application with permission to read the system log" and was sent to HTC through its "Tell HTC" error reporting tool." *Id.* The FTC noted the consumers had "little, if any, reason to know their information was at risk because of the vulnerabilities introduced by HTC." *Id.* ¶ 78. Ultimately, the FTC found that HTC had engaged in unfair or deceptive acts or practices in violation of the Federal Trade Commission Act given deceptive statements in its user manuals and user interface. *Id.* ¶ 79.

III. DISCUSSION

A. Legal Standard

Under Federal Rule of Civil Procedure 12(b)(6), a party may move to dismiss based on the failure to state a claim upon which relief may be granted. *See* Fed. R. Civ. P. 12(b)(6). A motion to dismiss based on Rule 12(b)(6) challenges the legal sufficiency of the claims alleged. *See Parks Sch. of Bus. v. Symington*, 51 F.3d 1480, 1484 (9th Cir. 1995). In considering such a motion, a court must take all allegations of material fact as true and construe them in the light most favorable to the nonmoving party, although "conclusory allegations of law and unwarranted inferences are insufficient to avoid a Rule 12(b)(6) dismissal." *Cousins v. Lockyer*, 568 F.3d 1063, 1067 (9th Cir.

2009). While “a complaint need not contain detailed factual allegations . . . it must plead ‘enough facts to state a claim to relief that is plausible on its face.’” *Id.* “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662 (2009); *see also Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556 (2007). “The plausibility standard is not akin to a ‘probability requirement,’ but it asks for more than sheer possibility that a defendant acted unlawfully.” *Iqbal*, 129 S.Ct. at 1949.

To the extent Plaintiffs’ claims sound in fraud, the SCAC must meet the heightened pleading standard of Federal Rule of Civil Procedure 9(b). *See Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009). Rule 9(b) provides: “In alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake. Malice, intent, knowledge, and other conditions of a person’s mind may be alleged generally.” Fed. R. Civ. P. 9(b). To satisfy Rule 9(b), the “complaint must ‘identify the who, what, when, where, and how of the misconduct charged, as well as what is false or misleading about the purportedly fraudulent statement, and why it is false.’” *Salameh v. Tarsadia Hotel*, 726 F.3d 1124, 1133 (9th Cir. 2013) (quoting *Cafasso, U.S. ex rel. v. Gen. Dynamics C4 Sys., Inc.*, 637 F.3d 1047, 1055 (9th Cir. 2011)). This encompasses the circumstances surrounding reliance. *See Kearns*, 567 F.3d at 1125 (holding that the complaint did not meet the standard of Rule 9(b) partly because the plaintiff failed to specify when he was exposed to the allegedly fraudulent advertisements, which ones he found material, and on which ones he relied).

B. Plaintiffs’ Standing to Assert Their Claims

In order to have Article III standing to assert a claim, a plaintiff must have suffered an injury-in-fact that is fairly traceable to the actions of the defendant, and that his injury is likely to be redressed by a favorable decision. *See, e.g., Ass’n of Public Agency Customers v. Bonneville Power Admin.*, 733 F.3d 939, 950 (9th Cir. 2013). Further, standing is “claim- and relief-specific, such that a plaintiff must establish Article III standing for each of her claims and for each form of relief sought.” *In re Adobe Systems, Inc. Privacy Litig.*, — F. Supp. 2d —, 2014 WL 4370016, at *10 (N.D. Cal. Sept. 4, 2014); *see also DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006)

1 (“[O]ur standing cases confirm that a plaintiff must demonstrate standing for each claim he seeks to
2 press.”). “In a class action, standing is satisfied if at least one named plaintiff meets the
3 requirements.” *Ollier v. Sweetwater Union High Sch. Dist.*, — F.3d —, 2014 WL 4654472, at *15
4 (9th Cir. 2014) (citation omitted). As discussed below, once a class is certified, standing may also
5 be established by members of the class.

6 The Device Manufacturers raise a number of challenges to Plaintiffs’ standing to bring the
7 various claims in the SCAC. Specifically, Defendants argue that: (1) Plaintiffs lack Article III
8 standing to assert their claims under California Penal Code § 502 (and related state consumer
9 protection statutes) as they have not alleged a sufficient injury-in-fact; (2) that Plaintiffs Cribbs and
10 Pipkin have failed to allege any injury; and (3) that Plaintiffs lack standing to assert claims under
11 state laws in which they do not reside and against Device Manufacturers who did not produce their
12 mobile devices. The Court addresses each argument in turn.

13 1. Plaintiffs Have Adequately Alleged Standing Under Cal. Penal Code § 502 and State
14 Consumer Protection Statutes

15 Defendants argue that Plaintiffs lack standing to assert a claim under the California
16 Consumer Data Access and Fraud Act (“CCDAFA”), Cal. Penal Code § 502, or any state consumer
17 protection statute because these statutory claims require proof that the Plaintiffs “suffer[ed] damage
18 or loss by reason of a violation.” Cal. Penal Code § 502(e). Plaintiffs respond, however, that they
19 have suffered damage in three ways: (1) diminished battery power and life in their mobile devices as
20 a result of the Carrier IQ Software; (2) alleged collection and disclosure of personal information; and
21 (3) they would not have purchased their mobile devices had they known the Carrier IQ Software was
22 installed. Plaintiffs have sufficiently alleged “damage” for purposes of the pleading stage by
23 alleging that the Carrier IQ Software diminished their mobile devices’ battery life and resources.
24 Accordingly, the Court need not address Plaintiffs’ alternative theories of damage and Defendants’
25 motion to dismiss on this ground is **DENIED**.

26 As detailed above, the SCAC has alleged, for each Plaintiff, that the Carrier IQ Software
27 “was installed and operating on his device, and taxing his device’s battery, processor, and memory,
28

1 as alleged herein.” *See* SCAC ¶¶ 8-25. Defendants contend that these “generalized” allegations are
2 “too vague and speculative” to establish Article III standing.

3 Defendants rely primarily on *Opperman v. Path, Inc.*, No. C13-0453-JST, 2014 WL 1973378
4 (N.D. Cal. May 14, 2014), for this proposition. In that case, plaintiffs alleged that installed malware
5 on their iDevices resulted in “diminished mobile device resources, such as storage, battery life, and
6 bandwidth.” *Id.* at *22. They alleged that the “unauthorized transmissions and operations used
7 iDevice resources, battery life, energy and cellular time at a cost to Plaintiffs and caused loss of use
8 and enjoyment of some portion of each iDevice’s useful life.” *Id.* The court found these allegations
9 insufficient, stating that because the plaintiffs had failed to “quantif[y] or otherwise articulate[] the
10 alleged resource usage, they fail to allege an injury that can serve as the basis of standing.” *Id.*

11 At the same time, other courts in this district have “found that unauthorized use of system
12 resources can suffice to establish a cognizable injury” when allegations plausibly suggested a non-de
13 minimis drain on those resources. *In re Google, Inc. Privacy Policy Litigation*, No. C12-01382-
14 PSG, 2013 WL 6248499, at *7 (N.D. Cal. Dec. 3, 2013). For example, in *In re iPhone Application*
15 *Litigation*, 844 F. Supp. 2d 1040 (N.D. Cal. 2012), the court found that plaintiffs had standing where
16 they had alleged “diminished and consumed iDevice resources, such as storage, battery life, and
17 bandwidth.” *Id.* at 1054. Plaintiffs further alleged that every time an application was downloaded,
18 personal information was sent to app developers and that Apple designed the iPhone to continually
19 send geographic location information to its servers. *Id.* at 1050. Similarly, in *In re Google Android*
20 *User Privacy Litig.*, 11-MD-02264 JSW, 2013 WL 1283236 (N.D. Cal. Mar. 26, 2013), plaintiffs
21 alleged that certain “spyware” had been installed in the Android OS and that this spyware tracked
22 and transmitted their geographic location. *Id.* *2. Plaintiffs alleged that these transmissions resulted
23 in a decrease to their device’s battery life “because the process of collecting geolocation data is
24 resource intensive and consumers battery life.” *Id.* at *2. While the court found the standing
25 question “close” because the plaintiffs had not alleged how frequently Google had collected the data
26 in question (and thus how often it used the device’s resources), it nonetheless found the allegation
27 sufficient for the pleading stage. *Id.* at *4, 5. Finally, in *Goodman v. HTC America, Inc.*, No. C11-
28 1793MJP, 2012 WL 2412070 (W.D. Wash. June 26, 2012), the court found allegations of drained

1 system resources sufficient for standing purposes where it was alleged that the defendant's
2 application collected, and sent, the user's geographic information every three hours or whenever the
3 mobile device's screen was refreshed. *Id.* at *7. The court found the alleged injury "both specific
4 and plausible." *Id.*

5 It is evident that where plaintiffs have alleged more than a "de minimis" injury to their
6 device's mobile resources as a result of "systemic rather than episodic" use of those resources,
7 standing will be found. *In re Google, Inc Privacy Litig.*, 2013 WL 6248499, at *7. Thus, in *In re*
8 *Google*, the court found a cognizable injury in fact had been alleged where plaintiffs claimed that
9 defendant uploaded the plaintiff's location information *every* time an application was downloaded
10 (with one plaintiff alleging that it occurred 27 times). *See id.*

11 The Plaintiffs' bare assertion that Carrier IQ "taxed" each Plaintiff's "battery, processor, and
12 memory" would likely be insufficient to state a sufficient injury-in-fact for standing purposes.
13 However, the SCAC provides further factual enhancement that makes Plaintiffs' allegations
14 plausible for purposes of the pleading stage. Specifically, the SCAC alleges that

15 Android developer Tim Schofield researched the presence of the
16 Carrier IQ Software on multiple Android smartphone platforms. He
17 has noted that in addition to the privacy issues, the embedded Carrier
18 IQ Software necessarily degrades the performance of any device on
19 which it is installed. The Carrier IQ Software is *always* operating and
20 *cannot be turned off*. It necessarily uses system resources, thus
21 slowing performance and decreasing battery life. As a result, because
22 of the Carrier IQ Software, in addition to having their private
23 communications intercepted, plaintiffs and prospective class members
24 are not getting the optimal performance of the mobile devices they
25 purchased, and which are marketed, in part, based on their speed,
26 performance, and battery life.

22 SCAC ¶ 85 (emphasis added) (citation omitted). Plaintiffs elsewhere in the SCAC repeat the
23 allegation that the Carrier IQ Software is always operating and cannot be turned off. *See, e.g. id.* ¶¶
24 40, 64, 74. Taking these allegations as true, and drawing all plausible inferences in Plaintiffs' favor,
25 the Court concludes that Plaintiffs have sufficiently alleged that the Carrier IQ Software has had a
26 "systemic," rather than "episodic," effect on the resources of Plaintiffs' mobile devices. This is
27 sufficient to plausibly allege standing at the pleading stage.
28

Defendants argue that Plaintiffs have failed to allege that the *specific functions* of the Carrier IQ Software that at issue had incremental effect on battery life or performance above and beyond the Software's legitimate uses. However, such an effect may clearly be inferred from the SCAC. As Plaintiffs have alleged that the Carrier IQ Software is always on, the continual operation of the Software in obtaining this information plausibly alleges and implies the Software has more than a de minimis impact on the battery life and performance of Plaintiffs' mobile devices. *See In re Google Android User Privacy Litig.*, 2013 WL 1283236, at *4-5; *Goodman*, 2012 WL 2412070, at *7.

Defendants motion to dismiss Plaintiffs' CCDAFA and other state consumer protection statute claims for lack of standing is accordingly **DENIED**.

2. Plaintiffs Cribbs and Pipkin's Standing

Defendants argue that Plaintiffs Cribbs and Pipkin do not have standing because the allegations in the SCAC affirmatively establish that they have not suffered any injury. They point to the allegations in Paragraph 53 of the SCAC which, quoting an AT&T letter to Senator Al Franken, states: "AT&T indicated further that the software 'also is embedded on the HTC Vivid, LG Nitro and Samsung Skyrocket devices, but has not been activated due to the potential for the software agent to interfere with the performance of those devices.'" SCAC ¶ 53. This is significant because Plaintiffs Cribbs and Pipkin are both alleged to have Samsung Skyrocket devices. *See* SCAC ¶¶ 9, 17. Defendants therefore contend that the Carrier IQ Software could not have caused Plaintiffs Cribbs and Pipkin any injury.

Plaintiffs respond that they have properly alleged that "Carrier IQ Software and related implementing or porting software was installed and operating on [their] device[s], and taxing [their] device[s'] battery, processor, and memory." *Id.* ¶¶ 9 17. They further argue that the quote Defendants rely upon was a "from AT&T's December 14, 2011 letter to Sen. Franken, and not a factual allegation from plaintiffs' experience or their counsel's investigation, which is ongoing." Docket No. 309, at 29.

Defendants are correct that the Plaintiffs' various allegations on this point appear to be in tension with each other. However, this tension is not fatal to Plaintiffs' standing at this stage of the proceedings. The allegations in the SCAC at Paragraph 53 quote a letter from AT&T. Taking all

inferences in Plaintiffs' favor, this letter suggests that AT&T chose not to activate the Carrier IQ Software on Samsung Skyrocket devices out of concerns for performance on those devices. There are no allegations in the SCAC, however, that Plaintiffs Cribbs or Pipkin used AT&T as their carrier. Given that the SCAC alleges that mobile carriers have the power to deactivate or remove the Carrier IQ Software, *see* SCAC ¶ 55 (Sprint indicating that it "began removing the Carrier IQ Software from mobile devices"), it is possible that the Carrier IQ Software was activated on Samsung Skyrocket devices used on mobile carriers other than AT&T. The allegations of the complaint must be taken as true and all reasonable inferences must be drawn in Plaintiffs' favor. So viewed, the Court concludes that Plaintiffs Cribbs and Pipkin have adequately alleged standing for purposes of the pleading stage. Whether the Carrier IQ Software was activated on their devices is a question properly directed at the summary judgment stage.

Defendants' motion to dismiss Plaintiff Cribbs' and Plaintiff Pipkin's claims for lack of standing is **DENIED**.

3. A Plaintiff's Standing to Assert Claims Under State Laws from States in Which He Does Not Reside and Against Defendants Who Did Not Manufacture His Device

Defendants' final argument is that this Court should dismiss for lack of standing any state law claims arising under the laws of a state in which no Plaintiff resides and as to devices not purchased by any named Plaintiff in states in which no Plaintiff resides. Defendants also argue that each individually named Plaintiff only has standing to assert claims against the Device Manufacturer who made his or her mobile device, and not those who manufactured phones purchased by others.

Plaintiffs have adequately alleged an injury-in-fact as to their individual state law claims for the reasons discussed above. As the Device Manufacturers have correctly pointed out, however, there is currently no named plaintiff who can assert an injury-in-fact arising under many of the state laws asserted; nor is there a named plaintiff who can assert certain state law claims against specific Device Manufacturers.⁵ While the putative class may be defined to include those with such

⁵ For example, there is one named Plaintiff from Illinois and it is alleged that he purchased an HTC EVO 4G – Luke Szulczewski. There are no named Plaintiffs from Illinois who are alleged to have purchased mobile devices from the other Device Manufacturers. Similarly, there is no named Plaintiff from, *inter alia*, Nevada.

standing, no class has yet been certified. *See In re TFT-LCD (Flat Panel) Antitrust Litig.*, No. M.07-1827 SI, 2011 WL 1753784 (N.D. Cal. May 9, 2011) (recognizing that ““putative class members are not parties to an action prior to class certification”” (quoting *Saleh v. Titan Corp.*, 353 F. Supp. 2d 1087, 1091 (S.D. Cal. 2004)). As discussed below, the critical question is whether the Court should adjudicate the standing question now at the pre-certification pleading stage as measured by the named plaintiffs only or, as Plaintiffs maintain, the Court should defer consideration of the standing question until after deciding class certification.

Given the prevalence of nationwide class actions, it is perhaps surprising that there is no Ninth Circuit precedent specifically deciding this question. *See Los Gatos Mercantile, Inc. v. E.I. DuPont De Nemours & Co.*, No. 13-cv-01180-BLF, 2014 WL 4774611, at *3 (N.D. Cal. Sept. 22, 2014) (“Surprisingly, there is no controlling case law on this issue.”). The Device Manufacturers contend, however, that *Easter v. American West Financial*, 381 F.3d 948 (9th Cir. 2004), is controlling and requires the Court to address its standing arguments at the initial pleading stage. In *Easter*, home loan borrowers sued a number of defendants alleging that they charged usurious mortgage interest rates – including defendants who had not harmed any of the named plaintiffs. In this precise circumstance – where certain defendants had been included in a lawsuit when *no* named Plaintiff had Article III standing to assert any claim against them – the Ninth Circuit noted (with almost no analysis or discussion) that the “district court correctly addressed the issue of standing before it addressed the issue of class certification.” *Id.* at 962. *Easter* stands for the unremarkable proposition that for a class action to proceed between the named parties, each named plaintiff must have standing to sue at least one named defendant; to hold each defendant in the case, there must be at least one named plaintiff with standing to sue said defendant. Without such threshold standing, the case (or that portion of the case) could not proceed. In *Easter*, there was no named plaintiff that was injured by and therefore had standing to sue a number of the defendants. Absent such threshold standing, it would be improper to allow the case to proceed to *e.g.*, class certification.

The case at bar is distinguishable. Unlike in *Easter*, here there is a named plaintiff in this suit who has Article III standing to assert a claim against each of the Device Manufacturers. This is what was missing in *Easter*: the threshold standing that might permit the case to proceed beyond the

1 initial pleading state to class certification did not exist in *Easter* as it does here. *Easter* did not
 2 address the question: Whether, once threshold standing is established, the Court has the power to
 3 certify the class before addressing the standing of unnamed class members. *Easter* did not broadly
 4 hold that district courts *must always* address standing issues before class certification.

5 Any doubt as to the limited scope of *Easter* holding was resolved in *Perez v. Nidek Co., Ltd.*,
 6 711 F.3d 1109 (9th Cir. 2013). There, the Ninth Circuit recognized this question was an open one,
 7 expressly declining to reach the “difficult chicken-and-egg question of whether class certification
 8 should be decided before standing.” *Id.* at. 1113-14. Indeed, the Supreme Court in *Gratz v.*
 9 *Bollinger*, 539 U.S. 244 (2003) noted that that there was “tension in [its] prior cases” as to whether
 10 differences between a named plaintiff’s claims and the unnamed class members’ claims should be
 11 treated as a standing issue or one of adequacy and typicality under Federal Rule of Civil Procedure
 12 23. *See id.* at 263 n.15; *see also id.* at 263 (“As an initial matter, there is a question whether the
 13 relevance of this variation [between use of race in undergraduate transfer admissions and use of race
 14 in graduate admissions], if any, is a matter of Article III standing at all or whether it goes to the
 15 propriety of class certification pursuant to Federal Rule of Civil Procedure 23(a).”). Commentators
 16 have made similar observations. *See* William B. Rubenstein, *Newberg on Class Actions* § 2.6 (5th
 17 ed.).

18 It is not surprising, therefore, that district courts across the country have split on whether
 19 standing questions in the class action context can be deferred until after class certification. *See, e.g.*,
 20 *Los Gatos Mercantile*, 2014 WL 4774611, *3-4 (noting the division and citing cases); *see also In re*
 21 *Refrigerant Compressors Antitrust Litig.*, No. 2:09-md-02042, 2012 WL 2917365 (E.D. Mich. July
 22 17, 2012) (“There is currently a split among federal courts as to . . . the question of whether standing
 23 can be considered prior to class certification in class action lawsuits.”).

24 Many courts – including a number of courts in this District – have refused to defer
 25 consideration of these issues, treating it as a threshold matter that should be addressed at the
 26 pleading stage. *See, e.g.*, *Los Gatos Mercantile*, 2014 WL 4774611, at *4; *see also Pardini v.*
 27 *Unilever United States, Inc.*, 961 F. Supp. 2d 1048 (N.D. Cal. 2013) (“[T]here is only one named
 28 plaintiff and she has not alleged that she purchased ICBINBS outside of California. Thus, Plaintiff

1 does not have standing to assert a claim under the consumer protection laws of the other states
2 named in the Complaint. This is a pleading defect amenable to determination prior to a motion for
3 class certification.”); *In re Flash Memory Antitrust Litigation*, 643 F. Supp. 2d 1133, 1164 (N.D.
4 Cal. 2009) (“A class cannot assert a claim on behalf of an individual that they do not represent.
5 Where. . . a representative plaintiff is lacking for a particular state, all claims based on *that* state’s
6 laws are subject to dismissal.”).

7 The courts in these case have attempted to generalize Article III principles. In *Los Gatos*
8 *Mercantile*, for instance, the court noted that where a complaint includes multiple claims “at least
9 one named class representative must have Article III standing to raise each claim” and that in a class
10 action “each claim must be analyzed separately, and a claim cannot be asserted on behalf of a class
11 unless at least one named plaintiff has suffered the injury that gives rise to that claim.” *Los Gatos*
12 *Mercantile*, 2014 WL 4774611, *4. Similarly, in *In re Ditropan XL Antitrust Litig.*, 529 F. Supp. 2d
13 1098 (N.D. Cal. 2007), the court relied on the proposition that named plaintiffs only have standing if
14 he can allege and show that, “they personally have been injured, not that injury has been suffered by
15 other, unidentified members of the class to which they belong and which thy purport to represent.”
16 *Id.* (quoting *Lewis v. Casey*, 518 U.S. 343, 347 (1996)). These courts have looked at claims brought
17 under the laws of states in which no named plaintiff resided and concluded that the *named plaintiff*
18 lacked standing to assert such claims. On the critical question of whether these standing principles
19 may be examined after certification (when the unnamed class members become parties to the suit),
20 these courts have read *Easter* broadly as requiring that standing considerations should be addressed
21 prior to class certification. *See, e.g., id.* at 1107 (dismissing plaintiffs’ argument that the
22 “determination of standing is premature prior to class certification” on the ground that *Easter* had
23 rejected this “exact argument”); *see also Fenerjian v. Nongshim Co., Ltd.*, — F. Supp. 3d —, 2014
24 WL 5685562 (N.D. Cal. Nov. 4, 2014) (“Class allegations are typically tested on a motion for class
25 certification, not at the pleading stage. However, the Ninth Circuit has stated that standing should be
26 addressed before class certification.” (citing *Easter*, 381 F.3d at 962)).

1 In addition, some courts have articulated prudential reasons for adjudicating these class-
2 oriented standing questions at the pleading stage. For example, in *In re Wellbutrin XL Antitrust*
3 *Litig.*, 260 F.R.D. 143 (E.D. Pa. 2009), the court stated:

4 The alternative proposed by the plaintiffs [deferring consideration
5 until class certification] would allow named plaintiffs in a proposed
6 class action, with no injuries in relation to the laws of certain states
7 referenced in their complaint to embark on lengthy class discovery
8 with respect to injuries in potentially every state in the Union. At the
conclusion of that discovery, the plaintiffs would apply for class
certification, proposing to represent the claims of parties whose
injuries and modes of redress would not share. That would present the
precise problem that the limitations of standing seek to avoid.

9 *Id.* at 155. The court declined to “indulge in the prolonged and expensive implications of the
10 plaintiffs’ position only to be faced with the same problem months down the road.” *Id.*

11 While the above cases are not without logical force, the Court concludes that a strict
12 categorical requirement that the standing analysis must precede class certification is unwarranted.
13 First, for the reasons stated above, *Easter* cannot be read so broadly. Its facts are narrow, and the
14 Supreme Court in *Gratz* and the Ninth Circuit in *Perez* have confirmed this is an open question.

15 Furthermore, the Supreme Court has expressly recognized that, in at least some cases, courts
16 may address class certification prior to resolving standing questions. In both *Ortiz v. Fibreboard*
17 *Corp.*, 527 U.S. 815 (1999) and *Amchem Products, Inc. v. Windsor*, 521 U.S. 591 (1997), the
18 Supreme Court held that the lower courts had properly addressed class certification first prior to
19 Article III standing questions. Specifically, the Court stated that because resolution of the
20 certification issues was “logically antecedent to the existence of any Article III issues, it is
21 appropriate to reach them first.” *Amchem*, 521 U.S. at 612; *see also Ortiz*, 527 U.S. at 831 (“Thus
22 the issue about Rule 23 certification should be treated first, ‘mindful that [the Rule’s] requirements
23 must be interpreted in keeping with Article III constraints’”). Both *Ortiz* and *Amchem*
24 involved a global settlement in asbestos class actions. Among the unnamed class members in both
25 cases were “exposure only” plaintiffs – individuals who had been exposed to asbestos but had not
26 yet experienced any physical injury. The Supreme Court in both cases stated that class certification
27 questions could be addressed first as they were “logically antecedent” to the standing questions. *See*
28 *Ortiz*, 527 U.S. at 831; *Amchem*, 521 U.S. at 612. These “logically antecedent” cases, although

1 arising under unusual contexts, demonstrate that the Supreme Court has not insisted upon a rigid
2 ordering where all standing questions must be determined prior to class certification; these cases
3 establish that the ordering of standing versus class certification is not driven by a rigid constitutional
4 command.

5 To be sure, the precise contours of the “logically antecedent” doctrine coined in *Ortiz* and
6 *Amchem* are subject to dispute, with at least one commentator noting that the concept has “caused a
7 great deal of mischief.” See Linda S. Mullenix, *Standing and Other Dispositive Motions After*
8 *Amchem and Ortiz: The Problem of “Logically Antecedent Inquiries*, 2004 Mich. St. L. Rev. 703,
9 707. The Northern District of Illinois has concisely summarized the three dominant approaches to
10 *Ortiz* and *Amchem*’s “logically antecedent” language as follows:

11 Some courts have taken an almost categorical approach, routinely
12 resolving class certification questions prior to conducting a standing
13 inquiry. Others have taken a “nuanced” approach, attempting to
14 fashion a governing principle to determine when class certification is
15 considered “logically antecedent.” Finally, some courts limit *Ortiz*
and *Amchem* to the “very specific situation of a mandatory global
settlement class,” and do not interpret those cases to require courts to
consider class certification before standing.

16 *In re Plasma-Derivative Protein Therapies Antitrust Litig.*, No. MDL 2109, 2012 WL 39766 (N.D.
17 Ill. Jan. 9, 2012). For the reasons discussed above, this Court concludes that a more nuanced reading
18 of the “logically antecedent” doctrine is required, a reading which affords flexibility in the court’s
19 management of the ordering of these issues.

20 A leading commentator has noted that “[m]ost courts have interpreted *Amchem* and *Ortiz*
21 narrowly, holding that those cases stand for a limited exception that class certification can be
22 considered before standing in global settlement-only mass tort class actions.” Rubenstein, *supra*, §
23 2:2 (5th ed.); see also *Hoffman v. UBS-AG*, 591 F. Supp. 2d 522, 531 (S.D.N.Y. 2008) (noting that
24 *Ortiz* is limited to the “unique context of global-mass settlements”). However, that commentator
25 recognizes that a “‘growing consensus’ among lower courts is that class certification should indeed
26 be decided first ‘where its outcome will affect the Article III standing determination.’” Rubenstein,
27 *supra*, § 2:2 (quoting *Winfield v. Citibank, N.A.*, 842 F. Supp. 2d 560, 574 (S.D.N.Y. 2012). As the
28 Seventh Circuit has noted:

once a class is properly certified, statutory and Article III standing requirements must be assessed with reference to the class as a whole, not simply with reference to the individual named plaintiffs. The certification of a class changes the standing aspects of a suit, because “[a] properly certified class has a legal status separate from and independent of the interest asserted by the named plaintiff.”

Payton v. County of Kane, 308 F.3d 673, 680 (7th Cir. 2002). The Ninth Circuit has similarly recognized that “once a class has been certified, ‘the class of unnamed persons described in the certification acquire[s] a legal status separate from the representative.’” *Bates*, 511 F.3d at 987 (quoting *Sosna v. Iowa*, 419 U.S. 393, 399 (1975)).

Indeed, a number of cases in this “growing consensus” have addressed this issue in the precise “sister state” law scenario raised in this case and found class certification to be logically antecedent to class considerations. For example, in *Hoving v. Transnation Title Ins. Co.*, 545 F Supp. 2d 662 (E.D. Mich. 2008), plaintiff brought a class action alleging that the defendant title insurance company overcharged its premium on title insurance. *See id.* at 664. Plaintiff resided in Michigan, but sought to represent a class of consumers harmed by the defendant in Michigan, Arizona, Colorado, Maryland, Minnesota, Missouri, New Jersey, and Washington. *Id.* The court recognized that it was undisputed that plaintiff had established standing under Michigan law. It then found that in order for him to represent the putative class, “he must establish that his claim is typical of those individuals whose claims arise under the laws of the other states and he can represent those individuals adequately.” *Id.* at 668. According to the court, this analysis was necessarily, and logically, antecedent to questions of standing:

For example, with the facts presented in the complaint, the plaintiff certainly could not file an individual suit only seeking relief under Arizona law; however, a member of his proposed class from that state likely would have suffered an injury that could be redressed under Arizona law. The defendant has not seriously challenged the plaintiff’s standing to assert his claims arising from the alleged overcharge on his own refinancing transaction. The question whether he has standing to proceed as a class representative will be subsumed in the class certification decision, but it the argument does not support the defendant’s requested dismissal presently.

Id. at 668. Similarly, in *Jepson v. Ticor Title Insurance Company*, No. C06-1723-JCC, 2007 WL 2060856 (W.D. Wash. May 1, 2007), the district court found that where a named plaintiff had

1 established individual standing, questions about the plaintiff's ability to represent a class consisting
 2 of residents from other states were logically antecedent to standing inquiries because "there [was] no
 3 question that the proposed class would have standing to assert non-Washington claims if it were
 4 certified." *Id.* at *1.

5 Because of the nature of class certification – a process wherein members of the class acquire
 6 legal status once a class is certified – standing may be established by looking to the rights and
 7 interests of the members of the certified class; *see Sosna v. Iowa*, 419 U.S. 393, 401 (1975)
 8 (although controversy was no longer alive as to the named plaintiff, "it remains very much alive for
 9 the class of persons she has been certified to represent."). Thus, class certification may, in a true
 10 sense of the term, be "logically antecedent" to standing.

11 The conclusion that it is permissible to decide class certification before determining standing
 12 to pursue claims of unnamed class members is consistent with Article III. Provided there is
 13 threshold standing for each named plaintiff, ordering the adjudication process so as to address who
 14 cognizable parties are in the case (*i.e.*, whether unnamed class members have legal status) before
 15 addressing standing does no violence to Article III. A case or controversy may still be assured once
 16 the class is certified.

17 This conclusion is also consistent with a body of cases that have examined the question
 18 whether a named plaintiff in consumer class action can bring suit on behalf of individuals who
 19 purchased products different from, but similar to, those purchased by the named plaintiff. In these
 20 cases, it could be argued that the named plaintiff would not have Article III standing to assert
 21 directly such claims against the defendant – having never purchased the "similar" product, he or she
 22 can not claim to have suffered an injury-in-fact from that product. Despite this fact, a growing
 23 number of courts in this District allow these putative class actions to proceed as to the "similar"
 24 product claims and leave for class certification the question of whether the named plaintiff can
 25 adequately represent a class of individuals who purchased the "similar" products. *See, e.g., Rojas v.*
 26 *General Mills, Inc.*, No. 12-cv-05099-WHO, 2014 WL 1248017, at *10 (N.D. Cal. Mar. 26, 2014);
 27 *Bruton v. Gerber Prods. Co.*, No. 12-cv-02412-LHK, 2014 WL 172111 (N.D. Cal. Jan. 15, 2014).
 28 *Clancy v. Bromley Tea Company*, No. 12-cv-03003-JST, 2013 WL 4081632 (N.D. Cal. Aug. 9,

2013) provides a cogent discussion of the reasoning underlying these cases. There, the court noted that “[t]ransmogrifying typicality or commonality into an issue of standing would undermine the well-established principles that ‘[i]n a class action, standing is satisfied if at least one named plaintiff meets the requirements,’ and that ‘[t]he class action is an exception to the usual rule that litigation is conducted by and on behalf of the individual named parties only.’” *Id.* at *5 (quoting first *Bates*, 511 F.3d at 985 and then *Wal-Mart Stores, Inc. v. Dukes*, 131 S. Ct. 2541, 2550 (2011)).

The court continued:

Deciding at the pleading stage that a plaintiff cannot represent a class who purchased any different products than the plaintiff seems unwarranted, at least on the facts of this case. A plaintiff has sufficiently “typical” claims to represent a class if his claims “are reasonably co-extensive with those of absent class members; they need not be substantially identical.” Whether products are “sufficiently similar” is an appropriate inquiry, but it does not relate to standing: a plaintiff has no more standing to assert claims relating to a “similar” product he did not buy than he does to assert claims relating to a “dissimilar” product he did not buy. Seen this way, analyzing the “sufficient similarity” of the products is not a standing inquiry, but rather an early analysis of the typicality, adequacy, and commonality requirements of Rule 23.

Id.; see also Rubenstein, *supra*, § 2.6 (recognizing that addressing these questions at class certification is preferable insofar as Rule 23’s requirements “are designed precisely to address concerns about the relationship between the class representative and the class” and “focuses a court on pragmatic factors in a familiar and accessible manner”). These cases further exemplify the principle that there is no rigid rule that precludes class certification from being addressed before standing issues.

Accordingly, for the reasons discussed, the Court finds that it has the discretion to defer questions of standing until after class certification. Indeed, a number of courts, regardless of which analysis they have undertaken first, have couched their decision as one of discretion. For example, in *United Food & Commercial Workers Local 1776*, — F. Supp. 3d —, 2014 WL 6465235 (N.D. Cal. Nov. 17, 2014), the court, in deciding to address class certification at the pleading stage, stated:

The Ninth Circuit has confirmed that district courts *can address* ‘the issue of standing before it addresse[s] the issue of class certification.’ I find that the weight of the persuasive authority *allows me to* determine standing at this juncture, and that efficiency considerations

1 militate against waiting until class certification to determine the scope
2 of this case.

3 *Id.* at *19 (emphases added); *see also In re Lithium*, No. 13-MD-2420 YGR, 2014 WL 4955377
4 (N.D. Cal. Oct. 2, 2014) (“[T]he Court observes that the question of whether a plaintiff may
5 represent a class of another state’s residents is not necessarily, or at least not only, an issue of
6 standing. Rather, it is amenable to analysis as a matter of *either* standing *or* class representation.”);
7 *Kassman v. KPMG LLP*, 925 F. Supp. 453 (S.D.N.Y. 2013) (“The Supreme Court has held that a
8 court *may defer* consideration of Article III standing until after class certification are ‘logically
9 antecedent’ to Article III concerns.” (emphasis added)). “Allows,” “can” or “may,” and similar
10 language is indicative of a court recognizing that it possesses the discretion to take a given action.

11 On the facts of this case, however, as to claims brought under 35 state laws, the Court
12 declines to exercise this discretion and opts, as a matter of case management, to require the Plaintiffs
13 to present a named class member who possesses individual standing to assert each state law’s claims
14 against Defendants. It does so for several reasons. First, the Court notes that the named Plaintiffs in
15 this action come from 13 different states. The number of consumers from 35 other states in which
16 state law claims are asserted is vast relative to the claims to which the named Plaintiffs have
17 standing. *Compare In re Target Corp. Data Sec. Breach Litig.*, — F. Supp. 3d —, 2014 WL
18 7192478 (D. Minn. Dec. 18, 2014) (permitting class certification to proceed, noting that, “this is not
19 a case where a single named plaintiff asserts the laws of a multitude of states in which that plaintiff
20 does not reside. Rather, there are 114 named Plaintiffs who reside in every state in the union save
21 four and the District of Columbia.”); *with Insulate SB, Inc. v. Advanced Finishing Systems, Inc.*, No.
22 13-2664 ADM/SER, 2014 WL 943224 (D. Minn. Mar. 11, 2014) (refusing to allow class
23 certification where single named plaintiff asserted claims arising under the laws of 22 states and
24 Puerto Rico). The Court has reservations of subjecting the Device Manufacturers to the expense and
25 burden of nationwide discovery without Plaintiffs first securing actual plaintiffs who clearly have
26 standing and are willing and able to assert claims under these state laws. The policy concerns
27 articulated by the court in *In re Wellbutrin XL Antitrust Litig.*, 260 F.R.D. at 155, apply with
28 particular force here. Moreover, given the breadth of the proposed class and the number of state law

claims asserted on behalf of the class, there is a meaningful risk that the requirements of class certification under Rule 23 may not be met or, if they are, subclasses may have to be created which would engender delay (adding that any new named plaintiffs would likely be subject to another round of discovery and further class certification motion practice). It makes sense to address standing to bring some 35 state law claims before class certification.

In sum, although the Court believes Article III allows the district court to exercise discretion in ordering the determinations of class certification and standing, the Court finds it appropriate in this case to address standing in advance of class certification. In so doing, the Court finds the named Plaintiffs do not have standing to assert claims from states in which they do not reside or did not purchase their mobile device.

However, as to the named Plaintiffs' ability to sue under their own laws Device Manufacturers from whom other named Plaintiffs bought devices, the Court will exercise its discretion to defer determination of standing until after class certification. In contrast to *Easter*, these Defendants are properly in the case (having allegedly sold a device to at least one named Plaintiff); the potential burden of adjudicating class certification will not impose the kind of expansive burden entailed in permitting plaintiffs to sue each defendant under the laws of 35 other states.

Accordingly, the motion to dismiss claims brought under the laws of Alaska, Arkansas, Colorado, Delaware, District of Columbia, Hawaii, Idaho, Indiana, Kansas, Louisiana, Maine, Massachusetts, Minnesota, Missouri, Montana, Nebraska, Nevada, New Jersey, New Mexico, North Carolina, New Hampshire, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Utah, Vermont, Virginia, West Virginia, and Wyoming is granted for lack of standing by the named Plaintiffs. The motion to dismiss named Plaintiffs' claim against each of the Defendant Device Manufacturers is denied without prejudice to renewal after the Court addresses class certification.

C. Plaintiffs' Federal Wiretap Act Claim

The Federal Wiretap Act ("Wiretap Act"), 18 U.S.C. § 2510-2520, "is designed to prohibit 'all wiretapping and electronic surveillance by persons other than duly authorized law enforcement

officials engaged in investigation of specified types of major crimes.” *Greenfield v. Kootenai County*, 752 F.2d 1387, 1388 (9th Cir. 1985) (quoting S. Rep. No. 1097, 90th Cong., 2d Sess.). Plaintiffs allege that the Defendants violated 18 U.S.C. § 2511(1)(a), which makes it unlawful for a person to:

“intentionally intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.”

Id. § 2511(1)(a). The Act defines the term “intercept” as the “aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” *Id.* § 2510(4). Under 18 U.S.C. § 2520, anyone who has been damaged by the interception or disclosure of their communications in violation of the Wiretap Act are entitled to: (1) any preliminary, equitable, or declaratory relief that may be appropriate; (2) statutory and punitive damages; and (3) reasonable attorney’s fees. *See* 18 U.S.C. § 2520(b).

Defendants argue that Plaintiffs’ Wiretap Act claims fail because (1) Plaintiffs fail to allege Defendants “intercepted” any communications, as that term has been defined and applied by the Ninth Circuit, (2) the Carrier IQ Software is not a “device” as required by the Wiretap Act; (3) many of Plaintiffs’ allegations do not involve “contents” of communications; and (4) Plaintiffs have not alleged that any of the Device Manufacturers “acquired” any electronic communications.

1. Plaintiffs Have Adequately Alleged an “Interception” for Purposes of the Wiretap Act

As discussed above, “intercept” is defined as the “aural or *other acquisition* of the contents” of a communication. 18 U.S.C. § 2510(4) (emphasis added). The term “acquisition” is not defined in the statute, but the Ninth Circuit, looking at the term’s “ordinary meaning” has defined it as the “act of acquiring, or coming into possession of.” *United States v. Smith*, 155 F.3d 1051, 1055 n.7 (9th Cir. 1998). It has further held that “[s]uch acquisition occurs ‘when the contents of a wire communication are captured or redirected in any way,’” *Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009) (quoting *United States v. Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1992)).

Central to Defendants’ arguments in this case, the Ninth Circuit has construed the Wiretap Act’s interception element as requiring that the defendant intercept the communication in questions *contemporaneously with transmission*. In *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir.

2002), the Ninth Circuit held that for an electronic communication to be “intercepted,” it must have been “acquired during transmission, not while it is in electronic storage.” *Id.* at 878; *see also United States v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir. 2003) (holding that “contemporaneous interception – *i.e.*, an acquisition during flight – is required to implicate the Wiretap Act with respect to electronic communications”). Accordingly, under this interpretation of the interception requirement, tapping into or otherwise gaining unauthorized access into an individual’s voicemail and retrieving a saved voicemail message would not constitute an “interception” under the Wiretap Act.

In *Konop*, the Ninth Circuit found that a narrow definition of “intercept” which required acquisition contemporaneous with transmission was most “consistent with the ordinary meaning of ‘intercept,’ which is ‘to stop, seize, or interrupt in progress or course before arrival.’” *Konop*, 302 F.3d at 878 (quoting *Webster’s Ninth New Collegiate Dictionary* 630 (1985)). However, the Court based its holding primarily on the difference in the way Congress originally chose to define “wire communications” and “electronic communications” in the Electronic Communications Privacy Act (“ECPA”) of which the Wiretap Act is part. Prior to the passage of the USA PATRIOT Act, “wire communications” were defined as:

any aural transfer made in whole or in part through the use of facilities for the transmissions of communications by the aid of wire, cable, or other like connection . . . and *such term includes any electronic storage of such communication.*

18 U.S.C. § 2510(1) (1998) (emphasis added). The definition of “electronic communications,” by contrast, did not include “storage” of electronic communications, but was (as it is now) limited to the “transfer” of data, signs, signals, writings, etc. *See Konop*, 302 F.3d at 877. Thus, while the Ninth Circuit in *United States v. Smith*, 155 F.3d 1051 (9th Cir. 1998) had held that a wire communication could be “intercepted” when it was in storage (for instance, when stored in voicemail), *see id.* at 1055-56, the *Konop* court concluded that an “electronic communication” (the kind of communication referenced in § 2511(1)(a)) must be “acquired during transmission, not while it is in electronic storage,” *Konop*, 302 F.3d at 878. This reasoning was bolstered by the fact that Congress, when it passed the PATRIOT Act and amended the Electronic Communications Protection Act

(“ECPA”), had been “aware of the narrow definition courts had given the term ‘intercept’ with respect to electronic communications and chose not to change or modify that definition.” *Id.* In fact, Congress made that narrow definition applicable to wire communications by removing the reference to “electronic storage of such communication” from the definition of wire communications. *Id.* Thus, the *Konop* court concluded, “Congress . . . accepted and implicitly approved the judicial definition of ‘intercept’ as acquisition contemporaneous with transmission.” *Id.*

Of course, the prime benefit of modern electronic communications is the tremendous, almost instantaneous, speed in which they can be transmitted. Further, transmission of these communications necessarily depend on electronic storage in a way that more “traditional” forms of communications (letters, telephone calls, and the like) did not. Given these aspects of electronic communications, some courts have suggested that the Wiretap Act’s applicability to modern forms of communications may be limited. *See, e.g., Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003) (“While Congress’s definition of ‘intercept’ does not appear to fit with its intent to extend protection to electronic communications, it is for Congress to cover the bases untouched.”). For example, in *NovelPoster v. Javitch Canfield Group*, No. 13-cv-05186-WHO, 2014 WL 3845148 (N.D. Cal. Aug. 4, 2014), the district court noted that “[g]iven the speed of email, the Wiretap Act’s application to that form of electronic communication is undoubtedly limited” and “[t]here is only a narrow window during which an E-mail interception may occur – the seconds or mili-seconds before which a newly composed message is saved to any temporary location following a send command.” *Id.* at *10 (quoting *United States v. Steiger*, 318 F.3d 1039, 1050 (11th Cir. 2003)). The *Konop* Court itself recognized that “the existing statutory framework is ill-suited to address modern forms of communication.” *Konop*, 302 F.3d at 874.

Case law in this circuit applying *Konop*’s “contemporaneous with transmission” requirement has revolved around e-mail and related communications. These cases have held that unauthorized access to e-mails stored on a server (such as an e-mail server) does not constitute an “interception” for purpose of the Wiretap Act. *See, e.g., Konop*, 302 F.3d at 875, 878 (holding that unauthorized access to a secure website did not constitute an “interception” of communications on that site); *see*

1 also *Theofel v. Farey-Jones*, 359 F.3d 1066, 1077 (9th Cir. 2003) (determining that e-mails stored on
2 an ISP's servers were in "electronic storage" and therefore acquisition by subpoena did not
3 constitute an interception). These cases generally stand for the proposition that once an e-mail has
4 been received by the destination server, a communication becomes "stored" and contemporaneous
5 interception is no longer possible. See *NovelPoster*, 2014 WL 3845148, at *11 ("[R]eading emails
6 that have already been received in an email account's inbox does not constitute 'intercept[ion]'
7 under the statute."); see also *Global Policy Partners, LLC v. Yesin*, 686 F. Supp. 2d 631, 638 (E.D.
8 Va. 2009) (holding a qualifying intercept can only occur "when an e-mail communication is
9 accessed at some point between the time the communication is sent and the time it is received by the
10 destination server"). It has not mattered that the recipient did not actually "open" or read the
11 communication prior to the purported interception or that the challenged acquisition occurred
12 "milliseconds" after receipt – if the e-mail was received by the destination server, it was no longer in
13 transmission. See *NovelPoster*, 2014 WL 3845148, at *11 ("Nor does it matter if the intended
14 recipient had not read the emails intended to reach that recipient before it was allegedly
15 intercepted."); see also *Bunnell v. Motion Picture Association of America*, 567 F. Supp. 2d 1148,
16 1154 (C.D. Cal. 2007) ("[T]he amount of time a message is in storage is immaterial. As such,
17 [defendant] could have received the forwarded messages in milliseconds or days, it makes no
18 difference.").

19 The common thread in these cases is that the challenged acquisition occurred *after the*
20 *transmission was completed* – the e-mail messages at issue were received by the destination server
21 and no further "movement" of the message was necessary. In contrast, the Carrier IQ Software at
22 issue in this case is alleged to operate on sent and received communications *during* the transmission
23 process. For example, the SCAC alleges that Mr. Eckhart (the individual who "broke" the story
24 regarding Carrier IQ's software) uploaded a video on YouTube in which he showed that the Carrier
25 IQ Software was "intercepting incoming SMS text messages" and "intercepting outgoing web
26 queries and search terms." SCAC ¶ 46. The "incoming" and "outgoing" qualifiers imply
27 interception during transmission (as opposed, for example, to an allegation that already "sent" or
28 "received" text messages were intercepted). Similarly, in describing how the CIQ Interface

operates, the SCAC alleges that it is a “layer of code” “designed to see, recognize and intercept a host of data and content” and then “send that material down to the IQ Agent for further processing and possible transmittals.” SCAC ¶ 63. The allegation that the CIQ Interface “sees” and “recognizes” certain activity and then sends it down to the IQ Agent suggests a continual process by which communications to and from the phone are being contemporaneously analyzed during the transmission process.

Further, reviewing the YouTube video cited in the SCAC contains additional support for the inference that the Carrier IQ Software operates contemporaneously with transmission.⁶ In the video, Mr. Eckhart sent a text message to his mobile device and subsequently reviewed the device’s system log to demonstrate how the Carrier IQ Software operated. The video appears to demonstrate that before the SMS text message even appeared on the mobile device, the mobile device first ran the code “dispatchWAPPushtoCIQ” and then “dispatchSmsToCIQ.” See Trevor Eckhart, *Carrier IQ Part #2*, http://youtube.com/watch?=T17XQI_AYNo (at 12:30) (last visited on October 22, 2014). The text message was then sent to com.htc.android.iqagent.action.smsnotify where the text of the message was displayed in plain text. Only after all this was done does the system log code suggest that the received text message sent to the end user’s “inbox.” *Id.*

Finally, the SCAC references and quotes from a media interview with a Carrier IQ executive. See SCAC ¶ 65. Included in this interview was the following exchange:

It seems there must be some sort of buffer of received text messages, or a cache. Am I right?

We receive this information in real time, so a text message comes in, we’ll look at it. Is it for us? No, discard. So within the software itself there’s this kind of fast process. We shouldn’t need to buffer this information.

You shouldn’t need to? Does that mean you categorically don’t do it?

⁶ The Court may properly consider the contents of the referenced YouTube video at the pleading stage. *Cf. United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003) (holding that a court may, at the pleading stage, consider “documents attached to the complaint, documents incorporated by reference in the complaint, or matters of judicial notice”). Here, the YouTube video was effectively incorporated by reference into the SCAC. See SCAC ¶¶ 46, 65.

I haven't had that question before. I can't think of a reason why we'd need to buffer it. *Because we're operating in real time*, we'll see the SMS come in. Is it for us? Yes, OK, let's deal with it. If not, discard. Just like letting the small fish go through the net, the same analogy applies.

http://www.theregister.co.uk/2011/12/02/carrier_iq_interview/?page=2 (last visited October 22, 2014) (emphases added). This description of "real time" processing by the Carrier IQ Software and analogizing the process to a fishnet through which the transmission passes further suggest that the Carrier IQ software operates contemporaneously with transmissions.

Nonetheless, Defendants argue that because it is undisputed that the Carrier IQ Software operated on communications that either had been received by a mobile device (in the case of received communications) or had not yet left the mobile device (in the case of sent communications), the communications at issue are, as a matter of law, in "storage" and thus outside of the Wiretap Act's provisions. At the hearing, Defendants repeatedly cited the fact that the ECPA defines "electronic storage" as:

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

18 U.S.C. § 2510(17). Defendants argue that because the communications were on the mobile device when the Carrier IQ Software operated, they were in "temporary, intermediate storage" as defined by the ECPA. In essence, Defendants' argument is premised on the contention that because the Carrier IQ Software operated on information located on a mobile device, it was, by default, in some form of temporary storage. Accordingly, Defendants conclude that the communications were, at the time the Carrier IQ Software operated on them, stored communications that could not, under *Konop* and *Theofel* be intercepted.

As an initial matter, the Court has serious reservations as to whether the underlying legal premise to Defendant's argument – that a communication in temporary, transient storage *as part of the transmission process* is a "stored communication" that cannot be intercepted – is correct. In *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005), the First Circuit, sitting en banc, directly

1 addressed this question. In that case, the defendant was Vice President of Interloc, Inc., an online
 2 rare and out-of-print book listing service. Interloc gave its book dealer customers an e-mail address
 3 and then acted as the e-mail provider. *Id.* at 71. The indictment against the defendant alleged that
 4 defendant:

5 directed Interloc employees to intercept and copy all incoming
 6 communications to subscriber dealers from Amazon.com
 7 Interloc’s systems administrator modified the server’s procmail recipe
 8 so that, before delivering any message from Amazon.com to the
 9 recipient’s mailbox, procmail would copy the message and place the
 copy in a separate mailbox that Councilman could access. Thus,
 procmail would intercept and copy all incoming messages from
 Amazon.com before they were delivered to the recipient’s mailbox,
 and therefore, before the intended recipient could read the message.

10 *Id.* at 70. Defendant moved to dismiss the indictment, arguing that because, at the time the
 11 “procmail recipe” operated on the e-mail messages, the “messages existed ‘in the random access
 12 memory (RAM) or in hard disks, or both, within Interloc’s computer system’” they were not
 13 “electronic communications” under the Wiretap Act, but rather, were in electronic storage. *Id.* at 71.
 14 The district court and a First Circuit panel agreed, but the en banc court reversed.

15 The First Circuit sitting en banc began by noting that the plain text of the ECPA did “not
 16 clearly state whether a communication is still an ‘electronic communication’ within the scope of the
 17 Wiretap Act when it is in electronic storage *during transmission*.” *Id.* at 76 (emphasis added).
 18 Then, after looking at the legislative history behind the definition of “electronic storage” (on which
 19 Defendants in this case rely), the court found that the “purpose of the broad definition of electronic
 20 storage was to enlarge privacy protections for stored data under the Wiretap Act, not to exclude e-
 21 mail messages stored during transmission from those strong protections.” *Id.* Specifically, the court
 22 determined that Congress intended the definition of “electronic storage” to protect, under the Stored
 23 Communications Act, “messages and by-product files that are left behind after transmission, as well
 24 as messages stored in a user’s mailbox” from unauthorized access. *Id.* at 77. Finally, the court
 25 concluded that the fact that Congress had, prior to the PATRIOT Act, chosen to define “wire
 26 communications,” but not “electronic communications,” as including communications in “electronic
 27 storage” to be insignificant:
 28

If the addition of the electronic storage clause to the definition of “wire communication” was intended to remove electronic communications from the scope of the Wiretap Act for the brief instants during which they are in temporary storage en route to their destinations – which, as it turns out, are often the points where it is technologically easiest to intercept those communications – neither of the Senate co-sponsors saw fit to mention this to their colleagues, and no one, evidently, remarked upon it. No document or legislator ever suggested that the addition of the electronic storage clause to the definition of “wire communication” would take messages in electronic storage out of the definition of “electronic communication.” Indeed, we doubt that Congress contemplated the existential oddity that Councilman’s interpretation creates: messages . . . briefly cease to be electronic communications for very short intervals, and then suddenly become electronic communications again.

Id. at 78. Rather, the court concluded that the addition of the “electronic storage” element to the definition of “wire communication” was merely meant to protect voicemail messages under the Wiretap Act (as opposed to the Stored Communications Act).

Based on its exhaustive analysis of the legislative history, the First Circuit rejected a “rigid ‘storage-transit dichotomy’” and found that a communication in “transient electronic storage that is intrinsic to the communication process for such communications” was not a stored communication for purposes of the ECPA. *Id.* at 79. Other courts have distinguished between “transitory” storage and later storage of a communication. *See, e.g., Fredrick v. Oldham County Fiscal Court*, No. 3:08-CV-401-H, 2010 WL 2572815 (W.D. Ky. June 23, 2010) (“Vincent must assert that Thacker and Skaggs intercepted the original e-mail transmission, rather than accessing it later while stored in his e-mail account or on a server.”); *Yessin*, 686 F. Supp. 2d at 638 (“Thus, interception includes accessing messages in transient storage on a server during the course of transmission, but does *not* include accessing the messages stored on a destination server.”).

This analysis is persuasive. Not only is *Councilman*’s analysis of legislative history thorough and convincing, to hold otherwise would make the Wiretap Act turn on the intricacies of a particular circuitry’s design: *e.g.*, whether there is cache memory – an engineering intricacy that has no evident relationship to the purposes of policies of the Wiretap Act.

Moreover, *Councilman* is consistent with the Ninth Circuit’s “contemporaneous” requirement articulated in *Konop*. The Ninth Circuit in *Konop* merely held that an interception under the Wiretap Act required acquisition “during transmission, not while it is in electronic

storage.” *Konop*, 302 F.3d at 87. *Konop*, *Theofel*, and every case cited by Defendants in this action involve situations where the transmission of the communication at issue had terminated and it had reached its *final destination*, even if only for a moment. *See id.* (addressing bulletins and postings on a secure website); *see also Theofel*, 359 F.3d at 1077 (addressing copies of e-mails *transmitted in the past* retained by the ISP). Thus, the matter transmitted had reached the storage stage as that term would be commonly understood. These cases, unlike *Councilman*, did not address whether an electronic communication can be “intercepted” when it is acquired in *transitory* electronic storage that is *part of the overall transmission process of* an electronic message.

To be sure, in footnote 6 of *Konop*, the Ninth Circuit addressed an argument raised by “dissent, amici, and several law review articles” that “the term ‘intercept’ must apply to electronic communications in storage because storage is a necessary incident to the transmission of electronic communications.” *Konop*, 302 F.3d at 878 n.6. These sources further argued that if the “term ‘intercept’ does not apply to the *en route* storage of electronic communications, the Wiretap Act’s prohibition against ‘intercepting’ electronic communications would have virtually no effect.” *Id.* The court responded to this argument by stating:

While this argument is not without appeal, the language and structure of the ECPA demonstrate that Congress considered and rejected this argument. Congress defined “electronic storage” as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof,” indicating that Congress understood that electronic storage was an inherent part of electronic communication.

Id. (quoting 18 U.S.C. § 2510(17)(A)). This statement in *Konop*, however, is *dicta*. The question of whether the term “interception” should apply to in transient “en route” storage stage of communication was not directly presented by the parties to the action, but was rather used by amici as support for the broader argument that because such temporary storage was inherent in all electronic communications, the “interception” requirement should apply to electronic communication in storage more generally. But, the communications at issue in *Konop* did not raise the issue of transitory “en route” storage. Rather, it examined only communications in permanent storage on a server *after* transmission – a factual scenario far afield from that presented by communications in transitory, temporary storage. Hence, the language quoted above was not a

1 holding of the court. *See, e.g., United States v. Pedregon*, 520 F. App'x 605, 608 (9th Cir. 2013)
 2 (“We are not bound by dicta – discussions that are ‘unnecessary to the Court’s holdings,’ – in
 3 decisions from our court or any other court.” (quotation omitted)). At least one decision in this
 4 District has applied both *Councilman* and *Konop*, implicitly finding no conflict between the
 5 decisions. *See, e.g., Garcia v. Haskett*, No. C05-3754 CW, 2006 WL 1821232, at *3 (N.D. Cal. June
 6 30, 2006) (“In order to constitute unlawful interception of electronic communication, the
 7 interception of email messages must have occurred while the messages were in a transient storage
 8 facility, not a place of permanent storage.”).

9 Accordingly, even if the Defendants are factually correct that the communications at issue in
 10 this case were in transitory storage on Plaintiffs’ mobile devices (such as the devices’ random access
 11 memory, cache memory, etc.) when the Carrier IQ Software operated on them, it is not at all
 12 apparent why there was no “captur[ing] or redirect[ing]” of these communications contemporaneous
 13 with their transmission. *Noel*, 568 F.3d at 749; *see also United States v. Symuszkiewicz*, 622 F.3d
 14 701 (7th Cir. 2010) (“Either the server in Kansas City or Infusino’s computer made copies of the
 15 messages for Szymuszkiewicz within a second of each message’s arrival and assembly . . . that’s
 16 contemporaneous by any standard.”).

17 Ultimately, however, the Court need not conclusively decide this issue for the simple fact
 18 that there are *no* allegations in the SCAC from which it can be established that the Carrier IQ
 19 Software operated on communications while they resided in such “storage.” *See, e.g., In re Yahoo*
 20 *Mail Litig.*, — F. Supp. 2d —, 2014 WL 3962824 (N.D. Cal. Aug. 12, 2014), (noting that
 21 defendant’s argument that its challenged practices only affected emails that had “already reached
 22 [its] servers” was a factual question contradicted by the complaint’s allegations that the defendant
 23 intercepted emails “while the emails are in transit” and “before placing the emails into storage”).
 24 Looking solely at the factual allegations of the SCAC, along with the materials incorporated by
 25 reference and discussed above, Plaintiffs have sufficiently alleged that the Carrier IQ Software
 26 intercepted communications contemporaneously with their transmission as required under the
 27 Wiretap Act.
 28

For the foregoing reasons, Defendants' motion to dismiss Plaintiffs' Wiretap Act claim on the grounds that Plaintiffs had failed to allege an interception contemporaneous with transmission is **DENIED.**

2. Plaintiffs May Only Rely on Alleged Interception of Text Messages and Internet Search Terms for Its Wiretap Act Claim

The definition of "intercept" under the Wiretap Act only applies to the interception of the "contents" of a communication. *See* 18 U.S.C. § 2510(4). "Contents," in turn, is defined as "includ[ing] any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8). In *In re Zynga Privacy Litig.*, 750 F.3d 1098 (9th Cir. 2014), the Ninth Circuit found that "record information regarding the characteristics of the message that is generated in the course of the communication" is not included in the definition of "contents." *Id.* at 1106.

Courts have excluded various types of information from the Wiretap Act's definition of "content." For instance, information about a telephone call's "origination, length and time" have been found to be non-content "record" information. *See United States v. Reed*, 575 F.3d 900, 917 (9th Cir. 2009); *see also Gilday v. Dubois*, 124 F.3d 277, 296 n.27 (1st Cir. 1997) (determining that a device that captured, *inter alia*, "the number called, and the date, time and length of the call" did not capture "contents" of any communication). Similarly, the geographic location of a mobile device at any given time has likewise been deemed to be non-content information. *See, e.g., Cousineau v. Microsoft Corp.*, 992 F. Supp. 2d 1116, 1127 (W.D. Wash. 2012) (holding that cell-site location information "does not constitute the contents of a communication under § 2510(8)"); *cf. In re Application of U.S. for an Order Directing a Provider of Elec. Comm'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 305-06 (3d Cir. 2010) (holding that cell phone user's location data is not "content" information for purposes of the Stored Communications Act).

The parties agree that Plaintiffs' allegations that the Carrier IQ Software intercepted text messages and URLs (to the extent the URLs contain a user's search terms) implicate "content" under the Wiretap Act. *See* Docket No. 311; *see also Zynga*, 750 F.3d at 1108-09 ("Under some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging a URL containing that search term to a third party could amount

1 to a disclosure of the contents of a communication.”). Additionally, Plaintiffs have not contended
 2 that data regarding a mobile device’s geographic location, the telephone numbers dialed or received,
 3 or applications purchased by a user implicate “contents” of communications as defined by statute.
 4 As a result, the parties only dispute on this ground is whether “user names” or “passwords” are
 5 content such that interception of this data falls under the Wiretap Act’s provisions. The Court
 6 concludes they are not.

7 User names as indicators of the identity of a user do not disclose the “substance, purport, or
 8 meaning” of any communication. Courts have, therefore, found comparable data to not be “content”
 9 information. For example, in *Zynga* the Ninth Circuit found that a user’s Facebook ID was mere
 10 record information, insofar as it simply functioned as a “‘name’ or a ‘subscriber number or
 11 identity.’” *Zynga*, 750 F.3d at 1107. Similarly, in *Svenson v. Google Inc.*, — F. Supp. —, 2014 WL
 12 3962820 (N.D. Cal. Aug. 12, 2014), plaintiffs had provided Google with their contact information
 13 (specifically their “name, email address, Google account name, home city and state, zip code, and in
 14 some instances telephone number”) as part of signing up for Google’s “Google Wallet” service. *Id.*
 15 at *1. Google, in turn, allegedly disclosed this information to third party app developers. *Id.* at *2.
 16 The court concluded this information was not “content” information because it was “the type of
 17 information that the Ninth Circuit recognized as record information in *Zynga*.”

18 At the hearing on Defendants’ motion to dismiss, Plaintiffs attempted to distinguish these
 19 cases by arguing that when a user transmits *both* a user name and password together, a substantive
 20 communication with the destination server is created. The “substance, purport, or meaning” of this
 21 communication, Plaintiffs’ contend, is the establishment of the user’s identity and a request for
 22 access, and that the interception of the user name and password results in the interception of the
 23 entire substance of the communication.

24 The Court is not persuaded. In *Zynga*, the Ninth Circuit cited with approval the First Circuit
 25 case, *Gilday v. Dubois*. There, plaintiff – an inmate in a Massachusetts prison – alleged that the
 26 prison’s system telephone monitoring and detailing regime violated the federal and Massachusetts
 27 wiretap act. Under the “detailing” system, the prison system recorded information such as the
 28 number called, the duration of the call, and the inmate’s PIN number (the number assigned to that

inmate that the inmate had to enter in order for the operator to complete the call). *Gilday*, 124 F.3d at 281. In finding no Wiretap Act violation, the First Circuit held, *inter alia*, that the “detailing” procedure did not fall within the ambit of the Wiretap Act because it “simply captures electronic signals relating to the PIN of the caller, the number called, and the date, time and length of the call.” *Id.* at 296 n.27. The PIN number in *Gilday* served the same function as a traditional user name and password under Plaintiff’s argument – authentication for purposes of access.

Just as interception of the PIN number in that case was found to not implicate “content” information, neither does interception of a user name or password. While such credentials may be a prerequisite to engaging in communications (i.e., entering a user name and password in order to access one’s email), the credentials themselves do not reveal the substance, purport, or meaning of any communication. Accordingly, the Court concludes that Plaintiffs cannot state a claim under the Wiretap Act for alleged interception of their user names or passwords by the Carrier IQ Software.

3. Plaintiffs Have Adequately Alleged that the Carrier IQ Software is a “Device” for Purposes of the Wiretap Act

As quoted above, the Wiretap Act defines interception as acquiring the contents of a communication “through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4). “Electronic, mechanical, or other device” is, in turn, defined as “any device or apparatus which can be used to intercept a wire, oral, or electronic communication” *except*:

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or ***(ii) being used by a provider of wire or electronic communication service in the ordinary course of its business***

Id. § 2510(5)(a) (emphases added). Defendants contend that the SCAC fails to properly allege that the Carrier IQ Software was a “device” for two reasons. First, Defendants argue that the SCAC alleges that the Carrier IQ Software is a “component” of the mobile devices and, second, that the Carrier IQ Software was used by the mobile carriers in their ordinary course of business.

1 Accordingly, the Defendants’ argue that, under § 2510(5)(a), the Carrier IQ Software is not an
2 “electronic, mechanical, or other device.”

3 As to the first argument, § 2510(5) does not exclude all “components” of a telephone or
4 telegraph instrument from the definition of “device.” Rather, relevant to this action, only
5 “components” that are used by a provider of electronic communications in the ordinary course of
6 their business are excluded. As discussed below, whether the Carrier IQ Software, as alleged, was
7 used by the mobile carriers in their “ordinary course of business” cannot be resolved at this stage.
8 Accordingly, Plaintiffs have sufficiently alleged that the Carrier IQ Software is a “device” for
9 purposes of the Wiretap Act.

10 In addressing the scope of the “ordinary course of business” exemption contained in
11 § 2510(5)(a), courts have noted that the modifier “ordinary” in the exemption means “not
12 everything [the provider] does in the course of its business would fall within the exception.” *In re*
13 *Google Inc. Gmail Litig.*, No. 13-MD-2430-LHK, 2013 WL 5423918, at *8 (N.D. Cal. Sept. 26,
14 2013). Stated another way, “not everything that a company may want to do falls within the
15 ‘ordinary course of business’ exception.” *Watkins v. LM Berry & Co.*, 704 F.2d 577, 582 (11th Cir.
16 1983).

17 Courts in this district have disagreed as to the precise contours of this exemption . On one
18 hand, the court in *In re Google Inc. Gmail Litigation* adopted a “narrow reading” of the exception,
19 and required that there be “some nexus between the need to engage in the alleged interception and
20 the subscriber’s ultimate business, that is, the ability to provide the underlying service or good.” *In*
21 *re Google*, 2013 WL 5423918, at *11. Under this reading, the exception “offers protection from
22 liability only where an electronic communication service provider’s interception facilitates the
23 transmission of the communication at issue or is incidental to the transmission of such
24 communication.” *Id.* at *8.

25 The legislative history of the ECPA provides some support for this narrow reading. Section
26 2511(2)(a)(i) protects from Wiretap Act liability any employee, officer, or agent of an electronic
27 communication service who intercepts, discloses, or uses that communication in the “normal course
28 of his employment while engaged in any activity which is a necessary incident to the rendition of his

1 service.” 18 U.S.C. § 2511(2)(a)(i). In addressing this (at the time) proposed liability exception, the
2 Senate Judiciary Committee stated:

3 [T]his provision reflects an important technical distinction between
4 electronic communications and traditional voice telephone service.
5 The provider of electronic communications services may have to
6 monitor a stream of transmissions in order to properly route, terminate,
7 and otherwise manage the individual messages they contain. These
8 monitoring functions, which may be necessary to the provision of an
9 electronic communication service, do not involve human listening in
10 on voice conversations. Accordingly they are not prohibited.

11 S. Rep. No. 541, 99th Cong., 2d Sess., *reprinted at* 1986 U.S.C.C.A.N. 3555, 3575. To be sure, this
12 report was addressing a distinct liability exception and used different language than that used in §
13 2510(5)(a)(ii) – “necessary incident to the rendition of” services as opposed to “ordinary course of
14 business.” Nonetheless, the report can be read as suggesting that “Congress intended to protect
15 electronic communication service providers from liability when the providers were monitoring
16 communications for the purposes of ensuring that the providers could appropriately route, terminate,
17 and manage messages.” *In re Google Inc. Gmail Litig.*, 2013 WL 5423918, at *10.

18 By contrast, the court in *In re Google, Inc. Privacy Policy Litigation*, No. C-12-01382-PSG,
19 2013 WL 6248499 (N.D. Cal. Dec. 3, 2013), rejected a narrow reading of the exception as requiring
20 that the challenged conduct be “necessary” to the provision of electronic communication services.
21 The court noted that Congress chose to use the broad term “business” – thus suggesting that the
22 exception “covers more far ranging activity.” *Id.* at *10. Thus, the court determined that the
23 “‘ordinary course of business’ exception is not limited to actions necessary to providing the
24 electronic communication services . . . at issue” but rather could also include actions taken by a
25 provider to further its “legitimate business purposes.” *Id.* at *11. *See also Berry v. Funk*, 146 F.3d
26 1003, 1009 (D.C. Cir. 1998) (noting that the activity in question must “be justified by a valid
27 business purpose” or “perhaps, at least . . . be shown to be undertaken normally”); *Kirch v. Embarq*
28 *Mgmt. Co.*, No. 10-2047-JAR, 2011 WL 3651359 (D. Kan. Aug. 19, 2011), *aff’d* 702 F.3d 1245
(10th Cir. 2012) (finding defendant’s “ordinary course of business” defense “appears to have merit,
as plaintiffs have admitted that Embarq conducted the NebuAd test to further legitimate business

1 purposes and that behavioral advertising is a widespread business and is commonplace on the
2 Internet”).

3 The Court finds that resolution of the question whether the § 2510(5)(a) exception should be
4 construed narrowly or broadly is unnecessary at the pleading stage in this case. In contending that
5 the Carrier IQ Software was used by mobile carriers in the ordinary course of their business, the
6 SCAC establishes the exception, even if broadly construed, does not apply.

7 Defendants cite to the letters sent by the various carriers to Senator Al Franken in response to
8 his questions regarding the use of the Carrier IQ Software. For example, they cite AT&T’s letter,
9 which stated:

10 We do not use [the Carrier IQ Software] to obtain the contents of
11 customers’ communications, to track where our customers go on the
12 Internet, or to track customer location. . . . AT&T must collect
operational data that can point to possible network upgrades, including
improved call completion rates.”

13 Docket No. 304-4, at 2 (cited at SCAC ¶ 53). Similarly, Sprint wrote to Senator Franken that

14 Sprint has not used Carrier IQ diagnostics to profile customer
15 behavior, serve targeted advertising, or for any purpose not
16 specifically related to certifying that a device is able to operate on
Sprint’s network or otherwise to improve network operations and
customer experiences.

17 Docket No. 304-5, at 3 (cited at SCAC ¶ 54). Defendants thus argue that it is undisputed on the face
18 of the SCAC that the Carrier IQ Software was used by the carriers as a diagnostic and
19 troubleshooting tool in the ordinary course of their business.

20 The problem with Defendants’ argument, however, is that even if the Carrier IQ Software
21 was used by the mobile service providers for legitimate business purposes (network diagnostics and
22 troubleshooting), Plaintiffs have alleged that the Carrier IQ Software has functionality (text message
23 and internet search term retrieval) that the phone carriers have expressly disclaimed. For instance, in
24 the same AT&T letter quoted above, AT&T stated that it did “not use CIQ to obtain the contents of
25 customers’ communications, to track where our customers go on the Internet, or to track customer
26 location.” Docket No. 304-2, at 2. Similarly, Sprint in its letter stated it did not receive the
27 “contents of the text messages” users received or sent or the “contents of users’ online search queries
28 from the Carrier IQ Software.” *Id.* at 4.

1 Plaintiffs have alleged, however, that the Carrier IQ Software intercepted both text messages
 2 and online search queries and Defendants have not explained how *this* functionality of the software
 3 either (1) “facilitates” or is “incidental” to the transmission of electronic communications to or from
 4 a mobile device (under the narrow reading of the exception) or (2) furthers the mobile carriers
 5 “legitimate” and ordinary business purposes (under the more broad reading of the exception). Given
 6 the allegations of the scope and inferences that must reasonably be drawn in Plaintiff’s favor
 7 regarding the functionality and use of the Carrier IQ Software, the Court cannot conclude on a
 8 motion to dismiss that the software qualifies as a component of a telephone system that is “being
 9 used as a provider of wire or electronic communication service in the ordinary course of its
 10 business,” even if that exception is broadly construed. *See, e.g., In re Google Gmail Litig.*, No. 5:
 11 13-MD-2430-LHK, 2014 WL 294441, at *3 n.2 (N.D. Cal. Jan. 27, 2014) (noting that “factual
 12 development would be necessary” to determine whether the challenged interceptions fit within the
 13 exception because the court “cannot determine based on the pleadings alone what is ‘necessary,’
 14 ‘customary or routine,’ or ‘instrumental’ to Google’s business”); *Shefts v. Petrakis*, No. 10-cv-1104,
 15 2012 WL 4049484 (C.D. Ill. Sept. 13, 2012) (finding a “genuine dispute of material fact” existed as
 16 to whether the challenged activities fell within the defendant’s “ordinary course of business”).

17 Finally, the Court has doubts as to whether the Device Manufacturers may even invoke the
 18 “ordinary course of business” exception codified at § 2510(5)(a)(ii). At least two courts have held
 19 that the exception *only* applies to the actual providers of communication services. *See, e.g., In re*
 20 *Google Gmail Litig.*, 2013 WL 5423918, at *11 (finding that the § 2510(5)(a)(ii) exception is narrow
 21 and was “designed only to protect electronic communication service providers”); *Shefts*, 2012 WL
 22 4049484, at *5 (“The ‘ordinary course of business’ exemption applies only to the provider of the
 23 communications service. . . . As only the ‘provider’ can use the device in order to fall into the
 24 exception, employees of the provider who are acting without authorization may not take advantage
 25 of it.”). The Device Manufacturers would not appear to fit within this statutory definition of a
 26 provider of wire or electronic communication services. *See* 18 U.S.C. § 2510(15) (defining
 27 “electronic communication service” as “any service which provides to users thereof the ability to
 28 send or receive wire or electronic communications”). Nonetheless, in light of this Court’s

determination that further factual development is needed to even determine if the use of the Carrier IQ Software was even in the mobile carrier's ordinary course of business, the Court need not resolve the precise question of whether a non-service provider can invoke the § 2510(5)(a)(ii) exception.

For the foregoing reasons, the Court concludes that Plaintiffs have alleged sufficient facts from which it may be inferred that the Carrier IQ Software is not used by electronic communication service providers in the ordinary course of their business. As a result, the Court concludes that the SCAC properly alleges that the Carrier IQ Software is an "[e]lectronic, mechanical, or other device" which "can be used to intercept a wire, oral, or electronic communication" 18 U.S.C. § 2510(5). Accordingly, Defendants' motion to dismiss on this ground is **DENIED**.

4. Plaintiffs Have Failed to State a Claim for Violation of the Wiretap Act Against the Device Manufacturers

Defendants' final argument against Plaintiffs' Wiretap Act claim is that Plaintiffs have failed to allege any "unlawful acquisition" of Plaintiffs' communications by the Device Manufacturers. As detailed above, the definition of "interception" requires "aural or other acquisition of the contents" of a communication. 18 U.S.C. § 2510(4). Defendants contend that Plaintiffs have not alleged that any Device Manufacturer "acquired" communications. The Court agrees.

The SCAC alleges that the Carrier IQ's customers – the individuals who would receive the information allegedly intercepted by the Carrier IQ Software – are "typically wireless carriers but sometimes device manufacturers." SCAC ¶ 68. There are simply no allegations – with the exception of HTC, discussed *infra* – that any Device Manufacturer actually received copies of Plaintiffs' text messages or internet search inquiries. In their opposition, Plaintiffs point to the fact that they "allege interception by the manufacturers throughout the SCAC" and that "acquisition" is a constituent element of the definition of "interception." Docket No. 309, at 37, 38. However, these conclusory allegations are insufficient to state a claim. *See, e.g., Cousins*, 568 F.3d at 1067 (noting that "conclusory allegations of law and unwarranted inferences are insufficient to avoid a Rule 12(b)(6) dismissal"). Further factual specificity is required under *Twombly* and *Iqbal*.

It is true the SCAC contains a myriad of allegations regarding HTC's acquisition of Plaintiffs' communications (including text messages) via the "Tell HTC" error reporting tool. *See*,

1 e.g., SCAC ¶ 72. However, the allegations in the SCAC do not support an inference that HTC's
2 acquisition was intentional – rather, it appears that HTC obtained the communications in question
3 through its error reporting tool as a result of it erroneously failing to deactivate “debug” mode in the
4 Android operating system, resulting in the communications being recorded in the system logs. At
5 the hearing on Defendants’ motion to dismiss, Plaintiffs indicated that it had received information
6 suggesting that Samsung committed a similar error and therefore received communications through
7 its error reporting tools.

8 While these allegations support a finding that two Device Manufacturers actually received
9 the contents of user’s communications, they nonetheless fail to establish liability under the Wiretap
10 Act. Liability under § 2511(1)(a) makes unlawful to “*intentionally* intercept . . . any wire, oral, or
11 electronic communication.” 18 U.S.C. § 2511(1)(a); *see also id.* § 2520(a) (creating civil liability
12 against a defendant who intercepts an electronic communication “in violation of this chapter”).
13 Because there are no factual allegations suggesting that HTC (or Samsung’s) acquisition of
14 communications was intentional, Plaintiffs have failed to plead a basis for Wiretap Act liability
15 against these Device Manufacturers. *See, e.g., Sunbelt Rentals, Inc. v. Victor*, — F. Supp. 2d — ,
16 2014 WL 4274313 (N.D. Cal. Aug. 28, 2014) (“Sunbelt did not intentionally capture or redirect
17 Victor’s text messages to the Sunbelt iPhone. . . . Given these circumstances, the requisite
18 intentional conduct is lacking.”); *see also Shubert v. Metrophone, Inc.*, 808 F.2d 401, 405 (3d Cir.
19 1990) (noting that the ECPA was amended to “underscore that inadvertent interceptions are not
20 crimes under the Electronic Communications Privacy Act”).

21 Plaintiffs additionally argue that the Device Manufacturers – as the entities that implemented
22 the Carrier IQ Software through their development of the CIQ Interface software – were
23 instrumental in the interception of Plaintiffs’ communications. Specifically, Plaintiffs contend that
24 the Device Manufacturers, by installing the Carrier IQ Software on its mobile devices, “caused” the
25 resulting acquisition – “[t]hey intercepted the plaintiffs’ text messages and Internet search terms . . .
26 by way of the software they wrote and placed on phones directed to consumers.” Docket No. 309, at
27 38. It is true that the SCAC contains sufficient factual allegations from which it can be inferred that
28 the Device Manufacturers were involved in the installation of the Carrier IQ Software on their

1 mobile devices. Again, however, there are no factual allegations that the Device Manufacturers
2 themselves “seized” or “redirected” any communications themselves. Rather, the SCAC alleges that
3 the Device Manufacturers provided a framework through which *other* parties – Carrier IQ and its
4 customers (typically wireless carriers) – were able to intercept communications.

5 Plaintiffs have failed to cite any case that would support the imposition of Wiretap Act
6 liability on a party who merely provided a means through which a third party subsequently
7 intercepts communications. To the contrary, authority has consistently rejected such a theory of
8 liability. For example, in *In re Toys R Us, Inc. Privacy Litigation*, No. 00-CV-2746, 2001 WL
9 34517252 (N.D. Cal. Oct. 9, 2001), Toys R Us had permitted a third party, Coremetrics, to place
10 software on its servers which loaded javascript code onto the computers of individuals who visited
11 Toys R Us’ website. *See id.* at *1. This code allegedly permitted defendants to “monitor, intercept,
12 transmit and record all aspects of a Webuser’s private activity when they access Toys R Us’
13 Webpages.” *Id.* The court dismissed plaintiffs’ claims against Toys R Us, finding that plaintiffs had
14 failed to allege that “Toys R Us itself intercepted, disclosed, or used plaintiffs’ electronic
15 communications.” *Id.* at *7.

16 Similarly, in *Kirch v. Embarq Management Co.*, customers of an ISP sued the ISP alleging
17 that it had hired a third party advertising company, NebuAd, Inc., to install NebuAd’s “Ultra-
18 Transparent Appliance” software (“UTA”) on the ISP’s networks. *Kirch*, 2011 WL 3651359, at *2.
19 This software tracked customers’ internet browsing habits and “built interest profiles based” on that
20 information. *Id.* The ISP routed all its internet traffic through the UTA and “furnished the
21 connection to the NebuAd equipment.” *Id.* at *4. As a result, the plaintiffs alleged that the ISP was
22 responsible for “connect[ing] its users to the UTA.” *Id.* Beyond this, the summary judgment record
23 suggested that the ISP had no involvement in the NebuAd System and did not have access to the
24 data collected. *Id.* The court rejected plaintiffs’ claims against the ISP, stating that “in order to
25 ‘intercept’ a communication, *one must come into possession or control of the substance, purport, or*
26 *meaning of that communication.*” *Id.* at *6 (emphasis added). The court noted that there was no
27 dispute that the ISP “had no access to that information or to the profiles constructed from that
28 information.” *Id.* Accordingly, because there was “nothing in the record that [the ISP] *itself*

acquired the contents of any communications as they flowed through its network,” the court concluded that the ISP could not be held civilly liable under the Wiretap Act. *Id.* (emphasis added).

Like the defendants in the above cases, there are no allegations that the Device Manufacturers in this case themselves acquired the contents of any of Plaintiffs’ communications. The closest the SCAC comes to tying the Device Manufacturers to the actual acquisition of communications is the assertion that “sometimes” unnamed Device Manufacturers were customers of Carrier IQ. *See* SCAC ¶ 68. This highly general, unsupported assertion is insufficient under *Twombly* and *Iqbal* to establish that the Device Manufacturers themselves acquired the contents of any communication, as opposed to merely providing an avenue through which Carrier IQ and the mobile carriers were able to effectuate such an interception. Such a conclusion is bolstered by the fact that the SCAC effectively alleges that the mobile carriers (not the device manufacturers) could choose what, if any, information they received from the Carrier IQ Software and could, if they wanted, remove the Carrier IQ Software from devices on their networks through system updates. SCAC ¶ 55 (Sprint indicating that it “began removing the Carrier IQ Software from mobile devices”).

Plaintiffs’ failure is significant because as there is simply no secondary liability (such as aiding and abetting) under the ECPA. *See, e.g., Byrd v. Aaron’s, Inc.*, — F. Supp. 2d —, 2014 WL 1327503 (W.D. Pa. Mar. 31, 2014) (“[S]econdary liability no longer exists under the current statutory structure of the ECPA.”); *Valentine v. WideOpen West Finance, LLC*, 288 F.R.D. 407 (N.D. Ill. 2012) (“As a general matter, courts have declined to find a private cause of action against those who aid and abet or conspire with others to intercept, disclose, or use electronic communications in violation of the ECPA.”). The Supreme Court has noted that when “‘Congress wishe[s] to create such [secondary] liability, it ha[s] little trouble doing so.’” *Central Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.*, 511 U.S. 164, 184 (1994). Accordingly, courts “should presume that Congress does not create a cause of action for aiding and abetting unless it specifically says so in the text.” *Wultz v. Islamic Republic of Iran*, 755 F. Supp. 2d 1, 57 (D.D.C. 2010); *see also Doe v. GTE Corp.*, 347 F.3d 655 (7th Cir. 2003) (“Normally federal courts refrain from creating secondary liability that is not specified by statute.”). The ECPA provision that creates

a civil cause of action for violation of § 2511 provides that “any person whose . . . electronic communication is intercepted . . . may in a civil action recover from the person or entity . . . which engaged in that violation.” 18 U.S.C. § 2520(a). As the Seventh Circuit held in *Doe*, nothing in this statute “condemns assistants, as opposed to those who directly perpetrate the act” and a “statute that is this precise about who, other than the primary interceptor, can be liable should not be read to create a penumbra of additional but unspecified liability.” *Doe*, 347 F.3d at 659.

Accordingly, Plaintiffs’ failure to allege sufficiently specific facts supporting a conclusion that the Device Manufacturers themselves intentionally intercepted Plaintiffs’ communications is fatal to their Wiretap Act claim against these defendants. However, the Court will afford Plaintiffs an opportunity to amend their complaint to cure this deficiency.

D. Plaintiffs’ State Privacy Law Claims

Defendants generally contend that Plaintiffs’ claims for violations of various states’ wiretap and/or privacy laws should be dismissed on the same grounds Defendants argued for dismissal of the Wiretap Act claim. *See* Docket No. 304, at 49. Accordingly, to the extent the Court has rejected Defendants’ arguments, *supra*, these arguments are likewise unavailing against the various state law claims which Defendants contend track the Wiretap Act.⁷ In addition, however, Defendants have raised separate arguments as to some of Plaintiffs’ state law wiretap claims based on unique features of those states’ laws. The Court addresses each of these arguments in turn.

⁷ Even if the Court had found Plaintiffs’ Wiretap Act claim defective as to warrant dismissal with prejudice, the Court would not have been inclined to summarily dismiss Plaintiffs’ state law wiretap claims simply on this basis. Defendants’ argument on this ground consisted of a single paragraph with a string cite of cases from the applicable states’ courts suggesting that some of these states’ wiretap acts are modeled after the Federal Wiretap Act and/or that state courts will look to Federal Wiretap Act claims as guidance. *See, e.g., State v. House*, 302 Wis. 2d 1, 11 (Wis. 2007) (“Wisconsin’s electronic surveillance statutes are patterned after Title III. Our interpretation of the state statutes therefore benefits from the legislative history and intent of Title III and from federal decisions considering Title III.”). Defendants’ blunderbuss approach, devoid of any actual analysis of each state’s laws, is insufficient to actually present an argument to this Court for resolution.

As a result, the Court only addresses those arguments Defendants specifically raised as to the various state law claims and declines to simply import any part of its above analysis of Plaintiffs’ Federal Wiretap Act claims into its holding regarding Plaintiffs’ state law claims.

1. Plaintiff Sandstrom's Claim under the Washington Privacy Act

Plaintiffs assert a claim under Washington's Privacy Act, Wash. Rev. Code § 9.73.060. SCAC ¶ 113(ee). Defendants argue that this claim fails because the Washington Supreme Court has interpreted the "intercept" requirement as requiring the complete stoppage of a transmission from reaching its intended audience and because the statute requires interception of a communication between two or more individuals. *See* Docket No. 304, at 50-51. Defendants further argue that to the extent Plaintiffs can state a claim under Washington's Privacy Act, such a claim must be limited to Plaintiffs' text messages and the numbers dialed and received. While the Court disagrees with Defendants' global challenge to Plaintiffs' Washington Privacy Act claim, it agrees that Plaintiffs may not rely on the full panoply of allegedly intercepted communications in support of its Washington claim.

a. Defendants Misread Washington Law Regarding the Requirements for an "Interception"

Washington Revised Code 9.73.30 makes it unlawful for any individual to "intercept, or record" any "[p]rivate communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication." Wash. Rev. Code 9.73.030(1)(a). To state a claim under this provision, a plaintiff must establish: (1) that a private communication was transmitted by a device; (2) this communication was intercepted or recorded; (3) by use of a device designed to record and/or transmit; (4) without the consent of all parties to the private communication. *State v. Roden*, 179 Wash. 2d 893, 898 (2014) (en banc).

In *Roden*, a police officer seized a criminal suspect's iPhone, looked through the text messages on the phone, and, posing as the suspect, sent and received a number of text messages with a third party in an attempt to set up a drug deal. *Id.* at 897. In addressing whether this constituted an "interception" of the text messages, the court noted that there was no statutory definition to guide its interpretation and, therefore, the term "intercept" should be given its ordinary meaning. *Id.* at 904. Relying on a dictionary definition, the court found that the "ordinary definition of 'intercept'" was "to 'stop . . . before arrival . . . or interrupt the progress or course.'" *Id.* (quoting *Webster's Third*

1 *New International Dictionary* 1176 (2002)). The court determined that the police officer's action
2 constituted an interception under this definition, analogizing it to an individual opening and reading
3 a letter in someone's mailbox before they received it. *Id.* at 905.

4 Relying on *Roden*, Defendants seek to import a limitation into Washington law that in order
5 for a communication to be intercepted, the intercepting party must completely prevent the intended
6 recipient of the communication from ever receiving it. *See* Docket No. 304, at 51 ("Plaintiff
7 Sandstrom, by contrast, does not, and cannot allege that the Carrier IQ software interrupted any
8 communications or stopped them from reaching him or the recipient to whom he directed them.")).
9 Defendants misread *Roden* and Washington law. While *Roden* involved a factual scenario where the
10 intended recipient never received the communications at issue, there is nothing in the decision to
11 suggest that the Washington Supreme Court was narrowly reading "intercept" as requiring such a
12 deprivation.

13 First, the "ordinary definition" adopted in *Roden* only speaks of stopping or interrupting the
14 progress of a communication – there is no modifier or limitation in this definition requiring that the
15 stoppage or interruption be permanent.

16 Second, adopting the reading of "intercept" advanced by Defendants would lead to the
17 absurd result that Washington's privacy law would not address an individual who eavesdropped on
18 telephone calls through the use of a listening device – the classic example of a "wiretap." The
19 purpose of eavesdropping is not to entirely prevent or interrupt a communication, but rather to
20 surreptitiously listen in on the communication. Numerous Washington courts have described
21 9.73.030 as preventing "eavesdropping" through electronic devices. *See, e.g., State v. Christensen*,
22 102 P.3d 789, 794 (Wash. 2004) (en banc) ("In 1967, the legislature amended [the privacy act] in
23 order to keep pace with the changing nature of electronic communications and in recognition of the
24 fact that there was no law that prevented eavesdropping."); *id.* at 794 n.3 ("Arguably, the most
25 significant piece of evidence about the extent to which the legislature intended to restrict
26 eavesdropping is the all-party consent requirement."). For example, in *State v. Faford*, 910 P.2d 447
27 (Wash. 1996) (en banc), an individual had used a police scanner eavesdrop on his neighbors cordless
28 telephone discussions and relayed information obtained to the police. *Id.* at 448. The court

determined the use of the scanner to eavesdrop on the neighbor's conversations constituted an "interception" and violated the privacy act. *Id.* at 452. The court so held despite the lack of any evidence that the eavesdropping resulted in the neighbors being unable to make or receive the phone calls at issue, an essential requirement for an interception under Defendants' reading of Washington law.

Third, even if Defendants were correct that their alleged actions could not constitute an "intercept," Washington Revised Code 9.73.030 prohibits both the interception *or recording* of private communications. There are sufficient allegations in the SCAC from which it can be inferred that the Carrier IQ Software effectively recorded (*e.g.*, the Carrier IQ Software code was observed processing a text message and displaying the text message in plain text) the challenged communications and transmitted the substance of those communications to either Carrier IQ and/or its customers. Such a recording and transmission would constitute a violation under 9.73.030.

Accordingly, the Court declines to dismiss Plaintiffs' Washington Privacy Act claim based on Defendants' proposed construction of Washington's "interception" requirement.

b. Plaintiff Sandstrom's Washington Privacy Act Claim May Only Extend to Alleged Interception of Text Messages and Phone Numbers Dialed and Received

Defendants second argument against Plaintiff Sandstrom's Washington Privacy Act claim is that this claim cannot extend to the alleged interception of any data other than text messages because the statute only applies to communications between two or more individuals. Docket No. 304, at 51. Defendants are correct, in part.

As quoted above, Washington's Privacy Act makes unlawful the interception or recording of private communications "transmitted by telephone, telegraph, radio, or other device between two or more individuals." Wash. Rev. Code § 9.73.030(1)(a). In *Cousineau v. Microsoft Corp.*, 992 F. Supp. 2d 1116 (W.D. Wash. 2012), the court found that Microsoft's interception of user's geo-location data was not covered under the Washington Privacy Act because "[u]nlike the federal SCA and Wiretap Act, the WPA requires a communication between at least two individual. . . . Without an individual on the other end of her communication (other than Microsoft), the transmission of

Cousineau’s data cannot be considered a communication under the WPA.” *Id.* at 1129. Similarly, in *State v. Gunwall*, 720 P.2d 808 (Wash. 1986) (en banc), the Washington Supreme Court held that a pen-register device that recorded the phone numbers dialed and received on a given line intercepted “private communications” for purposes of the act. The court reasoned:

The pen register is comparable in impact to electronic eavesdropping devices in that it is continuing in nature, may affect other persons and can involve multiple invasions of privacy as distinguished from obtaining documents in a single routine search warrant.

Id. at 816.

In light of *Cousineau* and *Gunwall*, the Court finds that Plaintiffs may base their Washington Privacy Act claim on the alleged interception of text messages and phone numbers dialed and received. Such information reflects communications “between two or more individuals” and therefore fits within Washington’s definition of interception. The alleged interception of other data – such as user’s geographical location, URLs, search terms, etc. – may not form the basis for liability under Washington’s Privacy Act as this data was not transmitted as part of a communication between individuals but instead directed to an automated system. Absent an interpretation from a Washington court to the contrary, such communication does not appear to be covered by the plain language of the Act.

2. Plaintiff Cline’s Claims Under Michigan’s Law

Plaintiffs assert a claim under Michigan’s eavesdropping statute, Mich. Stat. § 750.539c. SCAC ¶ 113(n). This provision states, in relevant part:

Any person who is present or who is not present during a private conversation and who wilfully uses any device to eavesdrop upon the conversation without the consent of all parties thereto, or who knowingly aids, employs or procures another person to do the same in violation of this section, is guilty of a felony

Mich. Stat. § 750.539c; *see also id.* § 750.539h (creating a private cause of action).

“Eavesdropping” is defined as “to overhear, record, amplify or transmit any part of the private discourse of others without permission of all persons engaged in the discourse.” *Id.* § 750.539a.

Defendants argue that this statute only covers the recording of “audible” communications and therefore does not apply to the type of electronic communications at issue in this case.

Defendants rely on the district court case of *Bailey v. Bailey*, No. 07-11672, 2008 WL 324156 (E.D. Mich. Feb. 6, 2008). In that case, defendant installed key logger software on his home computers to learn the passwords his wife used for her emails and private messaging accounts so that he could monitor his wife's (the plaintiff) internet communications. *Id.* at *1. Defendant eventually gave his divorce attorney copies of his wife's emails. After a highly contentious divorce and child custody hearing, plaintiff sued alleging, *inter alia*, a violation of Michigan's eaves dropping statute. The district court found that a "plain reading" of the eavesdropping statute demonstrated that it did not apply as the "key logger" software was not used in respect to a "conversation." *Id.* at *7. Rather, the court found that "[w]hen Plaintiff pressed the keys to enter her passwords, compose messages, or compose emails, she was not engaging in a conversation" because she was not in a "direct dialogue" with anyone else and the device did not record "the response on the other side." *Id.* at *8. The court then stated that "[t]he statute was meant to prohibit eavesdropping in the traditional sense of recording or secretly listening to *audible conversation[s]*." *Id.* (emphasis added). Reinforcing this interpretation, the court noted that:

the Michigan legislature felt the need to add a statute that deals specifically with the reading or copying of any message from a computer without authorization. Section 750.540 [discussed below] would be redundant if § 750.539c already prohibited the same.

Id. Accordingly, the court granted defendant summary judgment as to this claim.

Consistent with *Bailey*, Defendants' argue their narrow interpretation of § 750.539c is supported by the fact that another provision covers "tapping" electronic communications. Specifically, Mich. Stat. § 750.540(a) makes it a crime to "willfully and maliciously cut, break, disconnect, interrupt, tap, or make any unauthorized connection with any electronic medium of connection, including the internet or a computer, computer program, computer system, or computer network, or telephone." Section 750.540(b), in turn, bars an individual from "willfully and maliciously read[ing] or copy[ing] any message from any telegraph, telephone line, wire, cable, computer network, computer program, or computer system, or telephone or other electronic medium of communication that the person accessed without authorization." Unlike the eavesdropping statute at § 750.539c, there is no private cause of action or civil liability for a violation of § 750.540. *See*

1 *Bailey*, 2008 WL 324156, at *9 (“Here, § 750.540 does not expressly provide for a private cause of
2 action, and does provide for adequate enforcement by creating criminal penalties.”). Defendants
3 argue that if § 750.539c is construed to cover electronic communications such as those alleged in the
4 SCAC, § 750.540 will be rendered a nullity.

5 There are, however, Michigan state court cases that are in tension with the federal district
6 court’s narrow interpretation of § 750.539c. In *Lewis v. LeGrow*, 670 N.W.2d 675 (Mich. Ct. App.
7 2003), the Michigan Court of Appeals, despite noting that “eavesdropping [was] not at issue in this
8 case,” went on to state that eavesdropping under § 750.539c is “limited to overhearing, recording,
9 amplifying, or transmitting the private, oral, *or written* communications *of others* without the
10 permission of all persons engaged in the communication.” *Id.* at 683 (first emphasis added). The
11 court noted that the statutory definition of “eavesdropping” was limited to overhearing, recording,
12 amplifying, or transmitting the “private discourse of others.” *Id.* Because “discourse” was not
13 defined by statute, the court looked to its ordinary definition, which it found to be “communication
14 of thought by words; talk; conversation; . . . any unit of connected speech *or writing* longer than a
15 sentence.”” *Id.* (emphasis added) (quoting *Random House Webster’s College Dictionary* 384
16 (1992)).

17 Further, in the unpublished case of *Vollmar v. Laura*, No. 262658, 2006 WL 1008995 (Mich.
18 Ct. App. Apr. 18, 2006), the state court of appeals reviewed an eavesdropping claim in which
19 plaintiff alleged that defendant had improperly obtained copies of faxes intended for plaintiff. *See*
20 *id.* at *1. While the court ultimately affirmed the trial court’s summary judgment of the claim, it did
21 so on the basis that the facts did not “establish that defendants may be liable for the wilful use of any
22 electronic device to eavesdrop or that any of the defendants knew or should have known that the
23 copies of the facsimiles they received were obtained by the wilful use of a facsimile machine as an
24 eavesdropping device.” *Id.* at *2. This holding is significant because if § 750.539c is as narrow as
25 defendants (and the federal court in *Bailey*) suggest, the court could have simply affirmed summary
26 judgment on the ground that a fax is not an audible communication of the kind covered by §
27 750.539c.
28

The *Bailey* court's narrow interpretation of § 750.539c as only extending to eavesdropping on oral communications seems reasonable, given the substantial overlap that would exist between § 750.539c and § 750.540 if the former is construed as encompassing electronic communications. However, the court in *Bailey* cited no state court authority for its reading of the statute and did not address the Michigan Court of Appeal's statement in *Lewis* that the eavesdropping statute covered *written* communications. Given the apparent absence of state court authority supporting *Bailey*'s narrow construction of § 750.534c, and the indication from the Michigan Court of Appeals that such a construction would be unwarranted, the Court declines at this time to dismiss Plaintiffs' claims under Michigan's eavesdropping statute.

3. Plaintiff Szulczewski's Claim Under the Illinois Eavesdropping Law Fails

Plaintiffs assert a claim under Illinois' eavesdropping law, 720 Ill. Comp. Stat. § 5/14-2(a)(1). SCAC ¶ 113(g). Section 5/14-2 provides, in relevant part:

(a) A person commits eavesdropping when he:

(1) Knowingly and intentionally uses an eavesdropping device for the purpose of hearing or recording all or any part of any conversation or intercepts, retains, or transcribes electronic communication

(2) Manufacturers, assembles, distributes, or possesses any electronic, mechanical, eavesdropping, or other device knowing or having reason to know that the design of the device renders it primarily useful for the purpose of the surreptitious hearing or recording of oral conversations or the interception, retention, or transcription of electronic communications and the intended or actual use of the device is contrary to the provisions of this Article; or

(3) Uses or divulges . . . any information which he knows or reasonably should know was obtained through the use of an eavesdropping device.

720 Ill. Comp. Stat. § 5/14-2(a). Subsections (a)(1) and (a)(3), however, have been struck down as facially overbroad under the First Amendment by the Illinois Supreme Court in *People v. Melongo*, 6 N.E.3d 120 (Ill. 2014).

In *Melongo*, the defendant had a dispute with a court reporter regarding the accuracy of the court report's transcript. Eventually the court reporter referred the defendant to her supervisor, the

Assistant Administrator of the Cook County Court Reporter's Office. Defendant had a number of phone conversations with the administrator about his underlying dispute with the court reporter and surreptitiously recorded these conversations and then posted the recordings on her website. *See id.* at 122-23. Defendant was charged with violations of both § 5/14(a)(1) (for recording the conversations through an eavesdropping device) and § 5/14(a)(3) (for divulging the contents of the communications obtained through the use of an eavesdropping device). The Illinois Supreme Court affirmed the lower courts' finding that these two provisions were unconstitutional both on their face and as applied.

The court found that the statutes unconstitutional for several reasons. First, the court found that § 5/14(a)(1) (the "recording provision") criminalized a "wide range of innocent conduct" as it "criminalizes the recording of conversations that cannot be deemed private: a loud argument on the street, a political debate on a college quad, yelling fans at an athletic event, or any conversation loud enough that the speakers should expect to be heard by others." *Id.* at 126. Second, the court found that § 5/14(a)(3) (the "publishing provision") was also unconstitutional as "the plain language of this provision criminalizes the publication of any recording made on a cellphone or other such device, regardless of consent. This alone would seem to be sufficient to invalidate the provision." *Id.* at 127. Further, the court noted that under the United States Supreme Court's decision in *Bartnicki v. Vopper*, 532 U.S. 514 (2001), a "naked prohibition against disclosures" was "'fairly characterized as a regulation of pure speech' by an innocent party." *Melongo*, 6 N.E.3d at 127 (quoting *Vopper*, 532 U.S. at 526). Because the court had found that the "recording provision" of § 5/14(a)(1) was unconstitutional, the defendant's recordings could not be characterized as "illegally obtained" and therefore a prohibition on her disclosing those recording was unconstitutional.⁸

⁸ Prior to *Melongo*, the Seventh Circuit in *ACLU of Ill. v. Alvarez*, 679 F.3d 583 (7th Cir. 2012), in the context of a review of a preliminary injunction, found that the ACLU had a strong likelihood of prevailing on its First Amendment challenge to 720 Ill. Comp. Sta. § 5/14-2(a)(1). In its opinion, the Seventh Circuit noted that

Unlike the federal wiretapping statute and the eavesdropping laws of most other states, the gravamen of the Illinois eavesdropping offense is not the secret interception or surreptitious recording of a private communication. Instead, the statute sweeps much more broadly, banning *all* audio recording of *any* oral communication absent consent

1 In the SCAC, it appears that Plaintiffs intended to allege only a violation of § 5/14-2(a)(1).
 2 See SCAC ¶ 113(g) (“Ill. Comp. Stat. Ch. 720 § 5/14-6 provides the for the recovery in a civil action
 3 for relief for violations of *Ill. Comp. Stat. Ch. 720 § 5/14-2(a)(1)* . . .”). In light of the supervening
 4 *Melongo* decision, however, Plaintiffs no longer attempt to assert a claim under § 5/14-2(a)(1);
 5 instead, they contend that they can state a cause of action under § 5/14-2(a)(2) – the only substantive
 6 provision of § 5/14-2 not addressed by the court in *Melongo*. Plaintiffs assert that the Carrier IQ
 7 Software fits within this provision as it was “designed for the primary purpose of the surreptitious
 8 interception, retention, and transcription of electronic communication in contravention of the
 9 provisions of Article 14 of the Illinois Statutes.” Docket No. 309, at 44.

10 Even if the Court were to conclude that Plaintiffs had properly alleged a violation of § 5/14-
 11 2(a)(2) in the SCAC, Plaintiffs claim would still fail. As detailed above, a violation of § 5/14-
 12 2(a)(2) has three elements, the last of which is that the “intended or actual” use of the eavesdropping
 13 device manufactured or distributed by the defendant be “contrary to the provisions of this Article.”
 14 Complimenting this requirement is § 5/14-2(c), which expressly provides that

15 It is not unlawful for a manufacturer or a supplier of eavesdropping
 16 devices . . . to manufacture, assemble, sell, or possess an
 17 eavesdropping device within the normal course of their business *for*
purposes not contrary to this Article

18 720 Ill. Comp. Stat. § 5/14-2(c) (emphasis added). After *Melongo*, however, it is no longer unlawful
 19 to “[k]nowingly and intentionally us[ing] an eavesdropping device” to “hear[] or record[] any
 20 conversation” or to “intercept[], retain[], or transcribe[] electronic communication” – those
 21 provisions of § 5/14-2(c) have been struck as unconstitutional. 720 Ill. Comp. Stat. § 5/14-2(a)(1).
 22 Accordingly, even if Plaintiffs are correct that the Carrier IQ Software had as its primary purpose the
 23 “surreptitious interception, retention and transcription of electronic communication” (thus satisfying
 24
 25

26 of the parties regardless of whether the communication is or was
 27 intended to be private. The expansive reach of this statute is hard to
 28 reconcile with basic speech and press freedoms.

Alvarez, 679 F.3d at 595.

the first and second elements of § (a)(2)), such use could not be deemed to be lawfully “contrary to the provisions” of § 5/14-2 as required by the third element of § (a)(2).

Accordingly, the Court grants, with prejudice, Defendants’ motion to dismiss Plaintiffs’ claim under Illinois’ eavesdropping statute.

4. Plaintiffs’ California Comprehensive Data and Fraud Act Claim Will Be Dismissed With Leave to Amend

Plaintiff raises two distinct arguments as to why Plaintiffs’ claims under the California Comprehensive Data and Fraud Act (“CCDFA”), Cal. Pen. Code § 502, should be dismissed. First, they contend that Plaintiffs have failed to identify the precise provisions under which they are suing. Second, they argue Plaintiffs have failed to allege that Defendants, through the Carrier IQ Software, acquired communications by overcoming “technical or code based” measures. While, as explained below, the Court concludes that Plaintiffs should be required to affirmatively state which provisions of the CCDFA they allege Defendants have violated, the Court finds that Plaintiffs have adequately alleged that the Carrier IQ Software operates by circumventing technical or code based measures. Accordingly, while the Court will grant Defendants’ motion to dismiss the CCDFA claim, it will afford Plaintiffs leave to amend.

a. Plaintiffs Have Failed to Identify Which Provisions of § 502(c) They Allege Defendants Have Violated

California Penal Code § 502 enumerates nine different offenses relating to unauthorized computer access. Specifically, the act defines the following as a criminal offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

Cal. Penal Code § 502(c). Subsection 502(e) provides a private cause of action for any individual who suffers damage or loss as a result of a violation of one of these provisions. *See id.* § 502(e).

A review of § 502(c) reveals that at least some of these provisions clearly do not apply to the facts alleged in the SCAC. For example, there are no allegations in the SCAC that Defendants introduced a “contaminant” into a computer, computer system, or network. *Id.* § 502(c)(8). Similarly, Plaintiffs have not alleged that Defendants “disrupte[d] or cause[d] the disruption of computer services.” *Id.* § 502(c)(5). However, Plaintiffs never specify which provisions of § 502 they allege Defendants *did* violate. Rather, they generally allege:

Defendants have violated California Penal Code § 502 by knowingly accessing, copying, using, making use of, interfering, and/or altering plaintiffs’ and prospective class members’ data such as URL containing HTTP and HTTPS query strings embedded with information including search terms, user names, passwords, and granular geo-location information; granular geo-location information apart from that transmitted in URLs; text messages; telephone numbers dialed and received; other keystrokes; and application purchases and uses. Defendants acted on a systematic and continuous basis.

1 SCAC ¶ 105. In their opposition, Plaintiffs state that their allegations “borrow from the statutory
2 language found in Cal. Penal Code § 502(c)(1)-(9)” and are supported by all the facts alleged in the
3 SCAC. Docket No. 309, at 46.

4 Plaintiffs’ failure to specify the specific statutory basis for their § 502 action requires
5 dismissal. *See, e.g., I.B. v. Facebook, Inc.*, 905 F. Supp. 2d 989 (N.D. Cal. 2012) (“Plaintiffs do not
6 sufficiently allege which provision of the EFTA has been violated.”); *Balu v. Lake County*, No. C08-
7 3014 SI, 2008 WL 5234236 (N.D. Cal. Dec. 15, 2008) (“If plaintiff wishes to allege a § 1985 claim,
8 the amended complaint must identify under which subsection or subsections of § 1985 plaintiff
9 brings his claim”); *Brothers v. Hewlett-Packard Co.*, No. C06-02254 RMW, 2006 WL 3093685
10 (N.D. Cal. Oct. 31, 2006) (noting that under *Khoury v. Maly’s of California, Inc.*, 14 Cal. App. 4th
11 612 (1993), a claim alleging unfair business practices “must identify the particular section of the
12 statute that was violated”). Plaintiffs will, however, be granted leave to amend to specifically allege,
13 consistent with Fed. R. Civ. P. 11, which provisions of § 502(c) they contend Defendants’ conduct
14 has violated.

15 b. Plaintiffs Have Sufficiently Alleged that Defendants Acted “Without
16 Permission”

17 With the exception of § 502(c)(8), all of the prohibited conduct articulated in § 502(c)
18 requires that the defendant act “without permission”⁹ – a requirement that the California state courts
19 have yet to interpret. However, in *Facebook, Inc. v. Power Ventures, Inc.*, 844 F. Supp. 2d 1025
20 (N.D. Cal. 2012), a court in this District held that when a defendant “accesses [a] network in a
21 manner that circumvents technical or code-based barriers in place to restrict or bar a user’s access,
22 then the access does qualify as being ‘without permission.’” *Id.* at 1036. In that case, defendant ran
23 a website that allowed users to integrate their multiple social networking accounts into a single
24 experience and, as part of this service, users provided defendant with their Facebook login and

25
26 ⁹ As referenced above, it appears that § 502(c)(8) is inapplicable to this case as there are no
27 allegations that the Defendants have introduced a “contaminant” to a computer network. Further,
28 the definition of “contaminant” in the statute incorporates a permission requirement, so, in reality,
all of the conduct prohibited by § 502(c) requires a showing that the defendant acted “without
permission.” *See In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963, at
*13 (N.D. Cal. Sept. 20, 2011).

1 password. *Id.* at 1028. Facebook sued alleging that defendant’s service violated Facebook’s terms
 2 of use which required users to “refrain from using automated scripts to collect information from or
 3 otherwise interact with Facebook.” *Id.* In rejecting Facebook’s “violated terms of use” theory, the
 4 court stated:

5 The Court finds that interpreting the statutory phrase “without
 6 permission” in a manner that imposes liability for a violation of a term
 7 of use or receipt of a cease and desist letter would create a
 8 constitutionally untenable situation in which criminal penalties could
 9 be meted out on the basis of violating vague or ambiguous terms of
 use. . . . Thus, in order to avoid rendering the statute constitutionally
 10 infirm, the Court finds that a user of internet services does not access
 11 or use a computer, computer network, or website without permission
 12 simply because that user violated a contractual term of use.

13 If a violation of a term of use is by itself insufficient to support
 14 a finding that the user’s access was “without permission” in violation
 of Section 502, the issue becomes what type of action would be
 15 sufficient to support such a finding. The Court finds that a distinction
 16 can be made between access that violates a term of use and access that
 17 circumvents technical or code-based barriers that a computer network
 18 or website administrator erects to restrict the user’s privileges within
 the system, or to bar the user from the system altogether.

19 *Facebook, Inc. v. Power Ventures, Inc.*, No. C08-05780 JW, 2010 WL 3291750, at *11 (N.D. Cal.
 20 July 20, 2010).

21 Nothing in the *Power Ventures* decision held that overcoming “technical or code-based
 22 barriers” designed to prevent access was the *only* way to establish that the Defendant acted without
 23 permission. It merely held that access of a computer network that violated a provider’s “terms of
 24 service” was insufficient to establish lack of permission, while overcoming barriers erected
 25 specifically to prevent such access was sufficient to make this showing. Nonetheless, courts in this
 26 District have largely adopted this “overcoming technical or code based barriers” test as the operative
 27 test to determine if Defendant acted without permission even outside the context of an alleged
 28 violation of a term of service. *See, e.g., Sunbelt Rentals, Inc. v. Victor*, No. C13-4240 SBA, 2014
 WL 4274313 (N.D. Cal. Aug. 28, 2014) (“For purposes of Section 502, parties act ‘without
 permission’ when they ‘circumvent[] technical or code-based barriers in place to restrict or bar a
 user’s access.’”); *NovelPoster*, 2014 WL 3845148, at *9 (same); *Flextronics Int’l, Ltd. v. Parametric
 Tech Corp.*, No. 5:13-cv-0034-PSG, 2014 WL 2213910, at *4 (N.D. Cal. May 28, 2014) (“This

1 district has interpreted the phrase ‘without permission’ to require that the defendant have accessed
2 the computer system ‘in a manner that overcomes technical or code-based barriers.’”); *In re iPhone*,
3 2011 WL 4403963, at *12 (same).

4 Defendants argue that that Plaintiffs have not – and cannot – allege that Defendants acted
5 “without permission” by circumventing any technical or code based barriers to operate because the
6 Carrier IQ Software was “embedded on Plaintiffs’ devices at the point of manufacture” and, as such,
7 the software “operated as part of the normal operation of Plaintiffs’ phones.” Docket No. 304, at 55.
8 Despite the growing acceptance of the *Power Ventures* test in this District, the Court has
9 reservations as to whether this test correctly construes the term “without permission.” It is a
10 fundamental canon of statutory construction that unless a term is specifically defined by statute,
11 words will be interpreted as taking their “ordinary, contemporary, common meaning.” *Perrin v.*
12 *United States*, 444 U.S. 37, 42 (1979). “Permission” is defined as the “act of permitting” or “a
13 license or liberty to do something; authorization.” Blacks Law Dictionary 1176 (8th ed. 2004).
14 Similarly, the Ninth Circuit has, in the context of the federal Computer Fraud and Abuse Act,
15 defined the term “authorization” as meaning “permission or power granted by an authority.” *See*
16 *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009), (holding that an employer
17 gives an employee “authorization” to access a computer when the employer gives the employee
18 permission to use that computer). Holding that a defendant acts with “permission” for purposes of
19 the CCDFCA any time it does not need to overcome “technical or code based barriers in place to
20 restrict or bar a user’s access” leads to results which strain the plain and ordinary meaning of the
21 term “permission.”¹⁰

22 The cases upon which Defendants primarily rely demonstrate the seemingly perverse result
23 of such a construction. First, in *In re iPhone Application Litig.*, plaintiffs had downloaded

24
25 ¹⁰ By way of example, § 502(c)(2), makes it illegal, *inter alia*, for a defendant to
26 “[k]nowingly access and without permission take[], cop[y], or make[] use of any data from a
27 computer.” Cal. Penal Code § 502(c)(2). Under this provision, a defendant who acquires, copies, or
28 utilizes data from a computer without having obtained permission *for the acquisition, copying, or*
utilization of the data has violated the statute. Even if the defendant’s general “access” into the
computer system was with permission (as it was in *In re iPhone* and *Opperman*), the “without
permission” qualifier modifies the “tak[ing], cop[y]ing] or mak[ing] use of any data” action and must
be given force.

defendant's app and alleged that the application used code to access plaintiffs' "personal information on the iDevices without the user's permission or knowledge." *In re iPhone*, 2011 WL 4403963, at *2. Plaintiffs contended that defendant had "exceeded the scope of any authorization" that could have been granted at the time of purchase and that defendant had acquired the personal information "surreptitiously[ly]" and never secured plaintiffs' permission. Nonetheless, the court dismissed the § 502 claim, because "[o]n Plaintiffs' own allegations, the iOS and third party apps – which contain the alleged 'surreptitious code' – were all installed or updated *voluntarily* by Plaintiffs." *Id.* at *12. Similarly, in *Opperman v. Path, Inc.*, No. C13-0453-JST, 2014 WL 1973378 (N.D. Cal. May 14, 2014), plaintiffs contended that a number of app developers designed their applications to copy the user's Address Book information to its servers without the user's knowledge or consent. *Id.* at *3. Plaintiffs argued their CCDAFA claim was viable, notwithstanding the "technical or code based barrier" requirement, because they "did not know that the apps contained the malicious code at issue here." *Id.* at *21. The court rejected this argument: "Although Plaintiffs allege they did not grant permission to the apps to copy their address books, there is no suggestion that the apps overcame 'technical or code based barriers in place to restrict or bar a user's access.' According to the CAC, the apps in question had open access to Plaintiffs' address books." *Id.*

In neither of these cases can it truly be said, in an ordinary sense of the word permission, that the plaintiff gave "permission" to the app developer defendant to access their information in question. In fact, in both cases the offending app was alleged to have acted surreptitiously and, in the case of *Opperman*, the court acknowledged that plaintiffs had affirmatively alleged that they had never given the app permission to access the information in their devices' address books. That the plaintiffs had unquestionably downloaded the offending apps in question does not answer the question of whether the plaintiffs gave "permission" to the defendants to access and transmit their personal data. Yet *In re iPhone* and *Opperman* essentially held that a defendant who acts in the absence of permission does not act "without permission" – an anomalous and linguistically strained result. Instead, relying on *Power Ventures*, these cases required plaintiffs to show not only (1) that they did not give defendants permission to access and transmit to third parties their personal data, but also (2) that they had erected some form of technical or code based barrier to prevent such

1 access. The Court does not believe such a reading of the phrase “without permission” should be so
2 broadly construed so as to defeat Plaintiffs’ claims in this case. *See Weingand v. Harland Financial*
3 *Solutions, Inc.*, No. C11-3109 EMC, 2012 WL 2327660 (N.D. Cal. June 19, 2012) (this Court
4 previously noting that the *Power Ventures* court had not “base[d] its construction of § 502 on any
5 California state authority or on the statutory language”).

6 Plaintiffs have alleged that the Carrier IQ Software, and its operation, was “deeply hidden;”
7 that they had no notice was operating, and they had no way to remove the software or to opt-out of
8 its functionality. *See, e.g., SCAC ¶ 40.* Even under the *Power Ventures* test, the *Power Ventures*
9 court itself found “no reason to distinguish between methods of circumvention built into a software
10 system to render barriers ineffective and those which respond to barriers after they have been
11 imposed.” *Facebook, Inc. v. Power Ventures, Inc.*, 844 F. Supp. 2d 1025, 1038 (N.D. Cal. 2012).
12 *Id.* Given the background nature of the software and the fact it is continually operating (SCAC ¶
13 64), the Carrier IQ Software would effectively render any “technical or code based” barrier
14 implemented by the Plaintiffs ineffective. For example, if a user had placed a password on his
15 mobile device and received a text message or phone call, the Carrier IQ Software would, despite this
16 barrier, intercept the text message and/or the geographic location. Accordingly, at least in the
17 context which does not involve merely a violation of a term of service, Plaintiffs have alleged facts
18 from which it can be reasonably inferred that the Carrier IQ Software was “designed in such a way
19 to render ineffective any barriers the Plaintiffs might wish to use to prevent access” to their private
20 information. *In re Google Android Consumer Privacy Litig.*, No. 11-MD-02264 JSW, 2013 WL
21 1283236, at *12 (N.D. Cal. Mar. 26, 2013). This is sufficient to satisfy the “without permission”
22 requirement.

23 For the foregoing reasons, Defendants’ motion to dismiss Plaintiffs’ CCDFA claim for
24 failure to allege that Defendants circumvented a “technical or code based barrier” is **DENIED**.
25 Plaintiffs have adequately alleged that Defendants’ use of the Carrier IQ Software was “without
26 permission.”

E. Plaintiffs' Implied Warranty of Merchantability Claims

Plaintiffs' fifth cause of action alleges a breach of the implied warranty of merchantability under the laws of over thirty states and the District of Columbia against the Device Manufacturers. The Device Manufacturers have moved to dismiss these claims on a variety of grounds. First, Defendants argue that the implied warranty claims under California, Maryland, Michigan, New Hampshire,¹¹ Texas, and Washington law should be dismissed as Plaintiffs failed to afford them pre-suit notice of any alleged breach. Second, Defendants argue that Plaintiffs California-based implied warranty claims fail because Plaintiffs were not in privity with the Device Manufacturer and have failed to allege that they purchased their mobile devices in California. Finally, Defendants contend that Plaintiffs have failed to allege that their mobile devices were not "merchantable."

1. Effect of Plaintiffs' Alleged Failure to Provide Notice to Device Manufacturers

Defendants argue that Plaintiffs have failed to allege that they provided the Device Manufacturers pre-suit notice of their implied warranty of merchantability claims as required by California, Maryland, Michigan, New Hampshire, Texas, and Washington law.

Each of these states require a plaintiff seeking to assert a breach of implied warranty claim to provide the defendant with reasonable notice of the alleged breach. *See, e.g., Charter Oak Fire Ins. Co. v. JP & WJ, Inc.*, 230 F. App'x 650, 652 (9th Cir. 2007) (Washington law); *Tasion Communications, Inc. v. Ubiquiti Networks, Inc.*, No. C13-1803 EMC, 2014 WL 1048710, at *9 n.2 (N.D. Cal. Mar. 14, 2014) (California law); *Ingram v. Auto Palace, Inc.*, No. BPG-09-2660, 2012 WL 5077633 (D.Md. Oct. 17, 2012) (Maryland law); *Town of Hooksett Sch. Dist. v. W.R. Grace & Co.*, 617 F. Supp. 1265 (D.N.H. 1984) (New Hampshire law); *U.S. Tire-Tech, Inc. v. Boeran, B.B.*, 110 S.W. 3d 194, 198 (Tex. Ct. App. 2003) (Texas law). In general, the purpose of the notice requirement is "to allow the breaching party to cure the breach and thereby avoid the necessity of litigating the matter in court." *Donohue v. Apple, Inc.*, 871 F. Supp. 2d 913, 929 (N.D. Cal. 2012);

¹¹ The Court need not address arguments arising under New Hampshire law in light of the fact the only New Hampshire Plaintiff in this action is alleged to have been a resident of Michigan "at all pertinent times." *See supra* note 1. To the extent Plaintiffs seek to have Plaintiff Cline assert claims under the laws of both Michigan and New Hampshire, they shall, in the Third Consolidated Amended Complaint, allege facts establishing Plaintiff Cline's ability to assert such claims.

1 *see also, e.g., McKay v. Novartis Pharm. Corp.*, 751 F.3d 694, 705 (5th Cir. 2014) (holding, under
 2 Texas law, that failure to notify the seller of the breach “thereby allowing the seller an opportunity
 3 to cure, bars recovery on the basis of breach of warranty”); *Mattos, Inc. v. Hash*, 368 A.2d 993 (Md.
 4 Ct. App. 1977) (“A purpose of the notice requirement . . . was to inform the seller of a defect in the
 5 product, thus enabling him to correct the defect, if possible, and to minimize any damages.”).

6 Plaintiffs’ SCAC contains no allegations that Plaintiffs provided the Device Manufacturers
 7 notice of the alleged breach of the implied warranty of merchantability. Rather, the SCAC alleges
 8 that the Device Manufacturers had notice of Plaintiffs’ claims “by way of the individual suits that
 9 preceded filing of either consolidated amended complaint” or by way of “numerous reports of these
 10 breaches likely made to them directly” by third party press reports and the like. SCAC ¶ 342.

11 a. California Law Does Not Require Consumers to Provide Notice to Remote
 12 Manufacturers

13 The parties have cited conflicting case law on the question of whether California law requires
 14 a consumer to provide notice to a remote manufacturer with whom he has not dealt before filing a
 15 breach of warranty action. On one hand, Plaintiffs cite *Keegan v. American Honda Motor Co., Inc.*,
 16 838 F. Supp. 2d 929 (C.D. Cal. 2012), where the district court, relying on a line of California cases,
 17 found that “under California law, a consumer need not provide notice to a manufacturer before filing
 18 suit against them.” *Id.* at 951. On the other hand, Defendants cite to *Stearns v. Select Comfort*
 19 *Retail Corp.*, No. 08-2746 JF, 2008 WL 4542967 (N.D. Cal. Oct. 1, 2008) where the court held,
 20 without analysis, that a consumer had to provide notice to the entity that manufactured her allegedly
 21 defective bed. *See id.* at *5.

22 This Court has recently addressed this precise issue and concluded that California law
 23 required a *business entity* to provide notice to a remote manufacturer. *See Tasion*, 2014 WL
 24 1048710, at *5. It reaching this conclusion, however, the Court noted that the California Supreme
 25 Court had concluded that the “notice requirement . . . is not an appropriate one for the court to adopt
 26 in actions by injured *consumers* against manufacturers with whom they have not dealt.” *Id.*
 27 (quoting *Greenman v. Yuba Power Products, Inc.*, 59 Cal. 2d 57, 61 (1963)) (emphasis added). On
 28 this basis, citing federal district court cases involving consumers, the Court stated “federal district

1 courts in California have routinely held that plaintiffs are not required to provide pre-suit notice to a
2 remote seller/manufacturer with whom they have not dealt.” *Id.*

3 Defendants have provided no authority to cause this Court to reconsider its earlier ruling on
4 this issue in *Tasion*. Accordingly, insofar as the SCAC contains no allegations that the California
5 Plaintiffs are either sophisticated business entities or dealt with the Device Manufacturers directly,
6 the Court will not dismiss the California implied warranty claims on this basis.

7 b. Plaintiffs’ Maryland, Michigan and Texas Implied Warranty Claims Will Be
8 Dismissed for Lack of Notice

9 In their opposition, Plaintiffs contend that neither Maryland or Texas law requires that notice
10 be given to a remote manufacturer. With respect to Texas law, Plaintiffs are mistaken. In *U.S. Tire-*
11 *Tech*, the Texas Court of Appeals held that “a buyer is required to give notice of an alleged breach of
12 warranty to a remote manufacturer.” *U.S. Tire-Tech*, 110 S.W.3d at 199. In addition, this Court has
13 recently held that the weight of Texas authority required a breach of warranty plaintiff to provide
14 reasonable notice of any alleged breach to a remote manufacturer. *See In re MyFord Touch*
15 *Consumer Litig.*, — F. Supp. 2d —, 2014 WL 2451291, at *25 (N.D. Cal. May 30, 2014).
16 Michigan law holds similarly. *See Gorman v. American Honda Motor Co.*, 839 N.W.2d 223, 229-30
17 (Mich. Ct. App. 2013).

18 Plaintiff Cribbs is correct that Maryland law generally permits a buyer of goods to file a
19 breach of warranty claim against a remote manufacturer without providing that party notice. *See*
20 *Firestone Tire & Rubber Co. v. Cannon*, 452 A.2d 192 (Md. Ct. App. 1982). Nonetheless, in the
21 only decision to address this question under Maryland law, the District of Maryland held that a
22 remote manufacturer may raise as an affirmative defense a plaintiff’s failure to provide the required
23 notice to his *immediate* seller. *See Lloyd v. General Motors Corp.*, 575 F. Supp. 2d 714, 723 (D.
24 Md. 2008) (“[A] manufacturer has a distinct interest in whether an aggrieved consumer notifies his
25 immediate seller of a breach. It is only logical, therefore, that a consumer’s failure to observe this
26 requirement should provide the manufacturer with an affirmative defense.”); *but see Firestone Tire*

1 & *Rubber Co. v. Cannon*, 452 A.2d 192, 196 n.6 (1982) (declining to address whether a defendant
2 may raise a consumer’s failure to notify his immediate seller of an alleged breach of warranty).¹²

3 Accordingly, Maryland, Michigan, and Texas either require notice to a remote manufacturer,
4 or permit a remote manufacturer to assert the failure of Plaintiffs to afford notice to the immediate
5 seller. Accordingly, the Court must examine whether Plaintiffs have adequately alleged that they
6 provided reasonable notice either to the Device Manufacturers (Michigan and Texas) or to their
7 immediate seller (Maryland). The Court finds that they have not.

8 Courts applying the laws of these states have required *pre-suit* notice – accordingly, the
9 filing of a civil complaint cannot constitute “reasonable notice.” *See Lynx, Inc. v. Ordnance Prods.,*
10 *Inc.*, 327 A.2d 502, 514 (Md. Ct. App. 1974) (“Since the existence of a right of action is conditioned
11 upon whether notification has been given the seller by the buyer, where no notice has been given
12 prior to the institution of the action an essential condition precedent to the right to bring the action
13 does not exist and the buyer-plaintiff has lost the right of his remedy.”); *Gorman*, 839 N.W.2d at
14 229-30 (requiring “presuit notice of a breach-of-warranty claim”); *In re MyFord Touch*, 2014 WL
15 2451291, at *25 (N.D. Cal. May 30, 2014) (“Under Texas law, the filing of a complaint does not
16 constitute notice.”). Further, it is not sufficient that a defendant generally know of problems with
17 their products. Instead, a plaintiff must provide notice that he considers the defendant to be in
18 breach of the implied warranty. *See Lloyd*, 575 F. Supp. 2d at 723 (holding that the “notice of the
19 breach required is not of the facts, which the seller presumably knows quite as well, if not better
20 than, the buyer, but of the buyer’s claim that they constitute a breach.” (citation omitted)); *see also*
21 *McKay v. Novartis Pharm. Corp.*, 751 F.3d 694,706 (5th Cir. 2014) (holding that the notice must
22 “inform[] the seller that the transaction is claimed to involve a breach, and thus open[] the way for
23 normal settlement through negotiation”).

24 Accordingly, Plaintiffs’ reliance in their SCAC on the filing of complaints and Defendants’
25 generalized knowledge of complaints regarding the Carrier IQ Software as constituting notice of

27 ¹² Courts may address affirmative defenses at the motion to dismiss stage where an
28 affirmative defense “obvious on the face of a complaint,” *Rivera v. Peri & Sons Farms, Inc.*, 735
F.3d 892, 902 (9th Cir. 2013). For the reasons that follow, and based on the allegations in the
SCAC, Plaintiffs’ failure to provide their immediate seller notice is such a case.

1 their breach of warranty claim fails as a matter of law under the laws of Maryland, Michigan and
2 Texas. Accordingly, the Court will dismiss Plaintiffs' implied warranty claims arising under the
3 laws of these states.

4 c. The Court Will Not Dismiss Plaintiff Sandstrom's Washington Implied
5 Warranty Claim

6 Defendants have cited no Washington authority for either the proposition: (1) that an injured
7 consumer must provide notice to a remote manufacturer, or (2) that Washington requires any notice
8 to be provided prior to filing suit. Instead, the only case cited by Defendants applying Washington
9 law was a case out of this District where the court stated it was "not clear that pre-suit notice is an
10 absolute requirement under Washington law." *Donohue*, 871 F. Supp. 2d at 930. This Court's own
11 search has failed to locate any Washington case addressing whether notice to a remote manufacturer
12 is required or whether notice to a defendant must occur before filing suit. The lack of any on-point
13 authority is significant because the various jurisdictions in this country have reached differing results
14 on these questions. For example, while, as just discussed, Texas and Maryland require the *presuit*
15 notice, other jurisdictions allow the filing of a civil complaint to constitute the required notice for a
16 breach of warranty action. *See, e.g., Chemtrol Adhesives, Inc. v. American Mfs. Mut. Ins. Co.*, 537
17 N.E. 2d 624 (Ohio 1989) ("We decline to adopt such an absolute rule, as we believe in a proper case
18 the filing of a civil complaint could serve as notice of breach."); *see also Hearn v. R.J. Reynolds*,
19 279 F. Supp. 2d 1096, 1116 (D. Ariz. 2003) ("The Court finds that . . . filing a complaint upon an
20 opposing party (as is the case here) may constitute reasonably timely notice . . .").

21 Accordingly, the state of Washington law on the relevant questions is unclear. Further,
22 Defendants have failed to brief why, in the absence of this authority, the Court should nonetheless
23 construe Washington law as it suggests. For these reasons, the Court declines to dismiss Plaintiff
24 Sandstrom's implied warranty claim on this ground.

25 2. Plaintiffs' California Implied Warranty of Merchantability Claim Will Be Dismissed
26 for Lack of Privity, with Leave to Amend

27 Under California law, a plaintiff asserting a breach of implied warranty cause of action under
28 the commercial code must be in vertical privity with the defendant. *See, e.g., Clemens v.*

1 *DaimlerChrysler Corp.*, 534 F.3d 1017, 1023 (9th Cir. 2008) (“[A] plaintiff asserting breach of
 2 warranty claims must stand in vertical contractual privity with the defendant.”); *see also Paramount*
 3 *Farms, Int’l LLC v. Ventilex B.V.*, 500 F. App’x 586, 588 (9th Cir. 2012) (“Vertical privity, or in
 4 other words, privity of contract is required to sustain an implied warranty claim in California.”) .
 5 There are two potentially applicable exceptions to the vertical privity requirement. First, the third-
 6 party beneficiary exception generally provides that a consumer may, in certain circumstances, assert
 7 an implied warranty claim as a third party beneficiary of agreements between the manufacturer and
 8 retailer. In *In re MyFord Touch Consumer Litig.*, this Court held that this exception “remain[ed]
 9 viable under California law.” *In re MyFord Touch*, 2014 WL 2451291, at *31. Second, California
 10 courts have stated that while “direct dealings between a purchaser and manufacturer after the
 11 purchase are generally insufficient to create an exception to the privity requirement,” where the
 12 manufacturer “essentially adopts and benefits from the initial sales negotiations and there are
 13 numerous direct dealings between the parties, the requisite privity can be established.” *Cardinal*
 14 *Health 301, Inc. v. Tyco Electronics Corp.*, 169 Cal. App. 4th 116, a143 (2008).

15 Plaintiffs argue that they have met the privity requirement in three ways: First, they argue
 16 they purchased their mobile devices from actual or apparent agents of the manufacturers. *See* SCAC
 17 ¶ 336 (“[P]laintiffs and the class were in privity with the Device Manufacturers in that they
 18 purchased their mobile devices from actual or apparent agents of the Device Manufacturers, such as
 19 the Device Manufacturers’ authorized dealers.”). Second, they contend that they are third-party
 20 beneficiaries of a contract between the manufacturers and retailers. *See id.* ¶ 337 (“[P]laintiffs and
 21 the class were and are also in privity with the Device Manufacturers. . . . [P]laintiffs and the class
 22 members were intended third-party beneficiaries of the Device Manufacturers’ contract for sale of
 23 devices to the persons or entities from whom plaintiffs and the class ultimately purchased their
 24 mobile devices.”). Finally, Plaintiffs assert they had “direct dealings” with the manufacturer as a
 25 result of the written warranties the manufacturer provided in conjunction with the purchase of the
 26 mobile device.

27 The SCAC, however, contains no factual allegations to support any of these theories. For
 28 instance, short of the conclusory allegation that Plaintiffs purchased mobile devices “from actual or

1 apparent agents of the Device Manufacturers,” there are no factual allegations that any of the
 2 California residents in this action purchased their phones from such an agent. Nor are the factual
 3 elements of agency alleged. Similarly, Plaintiffs have failed to allege the facts of the underlying
 4 putative contracts for which they contend they are intended third-party beneficiaries. *Compare In re*
 5 *Toyota Motor Corp. Unintended Acceleration Marketing, Sales Practices & Products Liability*
 6 *Litig.*, 754 F. Supp. 2d 1145, 1185 (C.D. Cal. 2010) (noting that plaintiffs had “allege[d] facts
 7 tending to support that they are third-party beneficiaries”).

8 Finally, Plaintiffs’ attempt to invoke the “direct dealings” exception fails. Plaintiffs point to
 9 one fact in support of their argument that the direct dealings exception applies: “[P]laintiffs allege
 10 that the manufacturer provided written warranties in conjunction with the purchase of their mobile
 11 devices, and the written warranties are enforceable by plaintiffs and the class against the
 12 manufacturers” Docket No. 309, at 68 (quoting SCAC ¶ 337). However, the act of providing
 13 an express warranty to a consumer does not establish that the manufacturer has “numerous direct
 14 dealings” with that consumer. *See Cardinal Health*, 169 Cal. App. 4th at 143. Rather, Plaintiffs’
 15 argument on this point is precisely why California law does not impose a vertical privity
 16 requirement in breach of *express* warranty claims. *See id.* at 143-44 (“Privity is generally not
 17 required for liability on an *express* warranty because it is deemed fair to impose responsibility on
 18 one who makes affirmative claims as to the merits of the product, upon which the remote consumer
 19 presumably relies.”). As a court in this District has recognized, to allow the privity requirement in
 20 implied warranty actions to be “relaxed” any time a plaintiff has alleged reliance on an express
 21 warranty would be inconsistent “with clear California precedent that privity remains a requirement
 22 in implied warranty claims even though it has been eliminated in express warranty claims.” *See In*
 23 *re Sony PS3 Other OS Litig.*, No. C10-1811 RS, 2011 WL 672637, at *4 (N.D. Cal. Feb. 17, 2011).

24 Accordingly, Defendants’ motion to dismiss Plaintiffs’ implied warranty claim under Cal.
 25 Comm. Code § 2314 is **GRANTED**. Plaintiffs will be afforded leave to amend to plead sufficient
 26 facts, as opposed to legal conclusions, establishing that an exception to the vertical privity
 27 requirement exists.
 28

3. Plaintiffs' California Implied Warranty Claim Under the Song-Beverly Act Will Be Dismissed with Leave to Amend

In addition to asserting a claim for breach of the implied warranty of merchantability under the California Commercial Code, Plaintiffs also assert a claim for breach of the implied warranty under the Song-Beverly Consumer Warranty Act. SCAC ¶¶ 353-363. Unlike the implied warranty under the *Commercial* Code, there is no privity requirement under the Song-Beverly Warranty Act. *See In re MyFord Touch*, 2014 WL 2451291, at *29 (“For the implied warranty claim under the Song-Beverly Act, there is no privity requirement.”). However, the Song-Beverly Warranty Act *only* applies to consumer products purchased in California. *See Elias v. Hewlett-Packard Co.*, 903 F. Supp.2d 843, 851 (N.D. Cal. 2012) (“By its terms, the Song-Beverly Act applies only to goods sold in California.”). Here, while Plaintiffs allege a number of Plaintiffs reside in California there are actually no allegations in the SCAC that any of these Plaintiffs purchased their mobile devices *in California*. Plaintiffs, however, have cited documents suggesting that they will be able to allege that the California Plaintiffs purchased their mobile devices in California.

Accordingly, Defendant’s motion to dismiss Plaintiffs’ Song-Beverly Act claims will be **GRANTED** but Plaintiffs will be afforded leave to amend to allege where the California Plaintiffs purchased their mobile devices.

4. Plaintiffs Have Sufficiently Alleged that Their Mobile Devices Were Unmerchantable for Purposes of Their Implied Warranty Claims

Defendants substantively attack Plaintiffs’ implied warranty of merchantability claims alleging that Plaintiffs have not – and cannot – allege that the presence and operation of the Carrier IQ Software rendered their mobile devices unmerchantable. Docket No. 304, at 72. Defendants accordingly seek dismissal of Plaintiffs’ implied warranty claims arising under the laws of California, Maryland, Michigan, Mississippi, New Hampshire, Texas, and Washington.

Under the laws of each of these states, the implied warranty of merchantability warrants that a purchased good is “fit for the ordinary purposes for which such goods are used.” *See, e.g.*, Cal. Comm. Code § 2314(2)(c); Md. Code, Comm. Law § 2-314(2)(c); Miss. Code Ann. § 75-2-314(2)(c); N.H. Rev. Stat. § 382-A:2-314(2)(c); Tex. Bus. & Com. Code § 2.314(b)(3); Wash. Rev.

Code § 62A.2-314(2)(c). Courts across various jurisdictions have recognized that the concept of whether a product is “fit for ordinary purposes” necessarily “incorporates . . . the consumer’s reasonable expectations into the concept of merchantability.” *Robinson v. American Honda Motor Co., Inc.*, 551 F.3d 218 (4th Cir. 2009); *see also Venezia v. Miller Brewing Co.*, 626 F.2d 188, 190 (1st Cir. 1980) (“Under Massachusetts law the question of fitness for ordinary purposes is largely one centering around reasonable consumer expectations.”); *Denny v. Ford Motor Co.*, 662 N.E.2d 730, 736 (N.Y. 1995) (noting that the “fit for the ordinary purposes for which such goods are used” inquiry “focuses on the expectations for the performance of the product when used in the customary, usual and reasonably foreseeable manners”).

At the same time, the implied warranty of merchantability merely guarantees that the product will perform at a “minimum level of quality.” *Birdsong v. Apple, Inc.*, 590 F.3d 955, 958 (9th Cir. 2009). As such, the implied warranty “does not impose a general requirement that goods precisely fulfill the expectation of the buyer,” *Am. Suzuki Motor Corp. v. Superior Court*, 37 Cal. App. 4th 1291, 1296 (1995). Therefore, a product which “performs its ordinary function adequately does not breach the implied warranty of merchantability merely because it does not function as well as the buyer would like, or even as well as it could.” *Gen. Motors Corp. v. Brewer*, 966 SW.2d 56, 57 (Tex. 1998). Rather, the alleged defect in the product must be so fundamental as to render the product unfit for its ordinary purpose. *See Tietsworth v. Sears, Roebuck & Co.*, 720 F. Supp. 2d 1123, 1142 (N.D. Cal. 2010) (“The mere manifestation of a defect by itself does not constitute a breach of the implied warranty of merchantability. Instead, there must be a fundamental defect that renders the product unfit for its ordinary purpose.”).

Defendants contend that the “ordinary purpose” of mobile devices is communication – making and receiving phone calls, text messages, facilitating internet usage, and allowing usage of apps. Because of this, Defendants argue, Plaintiffs cannot establish that the Carrier IQ Software renders their mobile devices unfit for this ordinary purpose because there are no allegations that the software rendered the devices unable to make and receive phone calls, text messages, and the like. *See* Docket No. 304, at 73.

Defendants' definition of mobile devices' "ordinary purpose" finds some support in case law from courts in this District. Specifically, in *In re iPhone 4S Consumer Litig.*, No. C12-1227 CW, 2013 WL 3829653 (N.D. Cal. July 23, 2013), the court stated that the "iPhone 4S's intended and ordinary use is as a smartphone, 'which the court safely presumes includes functions like making and receiving calls, sending and receiving text messages, or allowing for use of mobile applications.'" *Id.* at *16 (quoting *Williamson v. Apple, Inc.*, No. 5:11-cv-0377 EJD, 2012 WL 3835104, at *8-9 (N.D. Cal. Sept. 4, 2012)). Notably, as this quote demonstrates, the court merely found that a mobile device's ordinary and intended use "includes" making and receiving calls, text messages, and the like, suggesting that the courts were not intending to provide an exhaustive definition of a mobile device's ordinary and intended use. *Cf. Dairy v. Bonham*, No. C-13-1519 EMC, 2013 WL 3829268, at *3 (N.D. Cal. July 23, 2013) ("[U]se of the word 'including' indicates the enumerated ways . . . is not exhaustive.").

Nonetheless, these courts have found that alleged defects which did not affect this core functionality did not render the mobile devices unfit for their ordinary purposes. For example, in *In re iPhone*, plaintiffs alleged that the iPhone was rendered unfit because Apple's "Siri" feature did not perform as advertised. 2013 WL 3829653, at *16. The court, however, found that this allegation failed to state a claim for breach of the implied warranty because plaintiffs had "not alleged that the iPhone 4S is deficient" in "making and receiving calls, sending and receiving text messages, or allowing the use of mobile applications." Rather, plaintiffs had alleged that the iPhone was deficient "in providing the Siri feature to access these functions." *Id.* Similarly, in *Williamson*, plaintiffs alleged that the glass on their iPhone was defective as it was easily scarred and broken, despite Apple's representations to the contrary. *See Williamson*, 2012 WL 3835104, at *1. The court rejected plaintiff's implied warranty claim, finding that the glass defect did not render deficient the iPhone's ability to make calls, send or receive text messages, or use mobile applications. *Id.* at *8. Finally, in *In re Google Phone Litig.*, No. 10-CV-0117-EJD, 2012 WL 3155571 (N.D. Cal. Aug. 2, 2012), plaintiffs did allege defects which touched on the core functionality of the Google phone – specifically, they alleged, *inter alia*, that the phone's 3G data connectivity was inconsistent and the phone occasionally dropped or missed phone calls. The court found, however, that plaintiffs had

1 failed to “demonstrate that this alleged defect is more than inconvenience” such that the phone was
2 unfit for its ordinary purpose. *Id.* at *5.

3 This Court finds that Defendants’ argument that the Carrier IQ Software does not render
4 Plaintiffs’ mobile devices unfit for the devices’ ordinary purpose simply because the devices could
5 make and receive phone calls, text messages, use mobile apps, and access the internet is overly
6 simplistic and underinclusive. While a defect must be “fundamental” to implicate the implied
7 warranty, “this does not mean the alleged defect must preclude any use of the product at all.”
8 *Stearns v. Select Comfort Retail Corp.*, No. 08-2746 JF, 2009 WL 1635931, at *8 (N.D. Cal. June 5,
9 2009). There are a number of examples of courts which have held that a defect can render a product
10 unfit notwithstanding the fact the product at issue could, in a technical sense, perform its base
11 function. These courts have found that the implied warranty can be breached when, although
12 capable of performing its ordinary function, the product nonetheless fails in a significant way to
13 perform as a reasonable consumer would expect.

14 Thus, in *Stearns*, plaintiffs alleged an implied warranty claim against a bed manufacturer on
15 the basis of mold growing on its beds. The court determined that the plaintiffs had adequately
16 alleged that the beds at issue “did not conform to expectations regarding ordinary use,” and simply
17 because “a person still may sleep on a moldy bed does not bar as a matter of law a claim for breach
18 of the implied warranty of merchantability.” *Id.* at *8. Similarly, in *Long v. Graco Children’s*
19 *Products Inc.*, No. 13-cv-01257-WHO, 2013 WL 4566763 (N.D. Cal. Aug. 26, 2013), plaintiff
20 alleged that defendants’ car seats contained a defective buckle that was “unreasonably difficult or
21 impossible to unlatch.” *Id.* at *1. Even though it was not disputed that the car seat provided
22 “adequate protective restraint” for the child, the court found plaintiffs adequately alleged the car seat
23 was unfit. *Id.* at *12. It held that “[c]onsumers do not merely expect a car seat to serve its bare-
24 minimum purpose” but rather would expect that they “would be able to quickly unlatch the harness
25 or buckle in case of an emergency.” *Id.* Finally, in *Isip v. Mercedes-Benz USA*, 155 Cal. App. 4th
26 19 (2007), a car manufacturer argued that so long as a vehicle provided transportation from point A
27 to point B, it necessarily was fit for its ordinary purpose. The court rejected this argument, finding it
28 to be an “unjustified dilution” of the implied warranty. Rather, it held that a vehicle that “smells,

lurches, clanks, and emits smoke over an extended period of time is not fit for its intended purpose. *Id.* at 27; *see also Fleisher v. Fiber Composites, LLC*, No. 12-1326, 2012 WL 5381381 (E.D. Pa. Nov. 2, 2012) (plaintiffs adequately alleged outdoor deck that became discolored by mold as a result of a defect was unfit for ordinary purpose as consumers expect outdoor decks to not only provide structural support, but to also to meet “a certain aesthetic expectation”).

The Court concludes that in determining if a defect rises to the level of rendering a product unfit for its ordinary purpose, the Court must ask two questions. First, the defect in question must be “fundamental” in that it affects the core functionality of the product. *See, e.g., Stearns*, 2009 WL 1635931, at *7 (requiring a “fundamental defect”). Thus defects which only affects functionality that is peripheral or tangential to the core function of the product – for example the strength of glass used in a mobile device or the effectiveness of Apple’s Siri function, *see, e.g., In re iPhone*, 2013 WL 3829653, at *16 – would be insufficient. In defining a product’s core functionality, a court should not seek to reduce a product to its most basic, bare minimum purpose, but rather should take a common sense view informed by reasonable consumers’ expectations about the function of the type of product in a general sense. *See Long*, 2013 WL 4566763, at *12 (rejecting “bare-minimum” view of a car seat’s purpose in light of consumer expectations); *see also Robinson.*, 551 F.3d at 224 (“This definition of merchantability incorporates trade quality standards and the consumer’s reasonable expectations into the concept of merchantability.”). Thus, the core function of a vehicle is not to provide transportation, it is to provide safe and reliable transportation, *see Isip*, 155 Cal. App. 4th at 27, and the core function of a bed is not simply to provide a place on which an individual can sleep, but rather to provide a place where an individual can sleep that is free from mold, *see Stearns*, 2009 WL 1635931, at *7. Second, just because a defect affects the core functionality of a product does not automatically mean that the product is unfit for its ordinary purposes. Rather, as discussed, the implied warranty only ensures that a product will meet a “minimum level of quality.” *Birdsong*, 590 F.3d at 958. The impairment of the core functionality must be significant enough to prevent the product from reaching a reasonably expected minimum level of quality.

On this basis, the Court finds, for purposes of the motion to dismiss, that Plaintiffs have adequately alleged that the Carrier IQ Software rendered their mobile devices unmerchantable.

1 While there is no dispute that the Carrier IQ Software did not make it impossible for Plaintiffs to
2 make and receive phone calls, text messages, and the like on their devices, that alone is not
3 dispositive. Consumers have a reasonable expectation that mobile devices, in general, will allow
4 them to communicate with others without having a third party surreptitiously intercept and transmit
5 those communications to third parties. Stated another way, it is beyond controversy that individuals
6 have a reasonable expectation of privacy as to the contents of communications made with their
7 mobile devices. *Cf. Riley v. California*, 134 S. Ct. 2473, 2489-91 (2014) (discussing the privacy
8 interests at stake in searches of cell phones by law enforcement and recognizing the user's
9 expectation of privacy). Just as a consumer would likely choose not to sleep on a bed contaminated
10 with mold, a consumer would likely choose to not use a mobile device that actively intercepted his
11 or her private communication data and potentially share that data with third parties.

12 Plaintiffs have, in the SCAC, provided sufficient factual allegations for the Court to
13 conclude, at this stage, that the Carrier IQ Software intercepts and/or transmits personal
14 communication data to third parties. *See, e.g., SCAC* ¶¶ 65, 68 (alleging that the Carrier IQ Software
15 intercepts and transmits to Carrier IQ and its customers data that can include URLs which contain
16 internet search terms, user names and passwords; text messages; app purchases and uses; a user's
17 keystrokes; numbers dialed and received; etc.). Taking all inferences in favor of the Plaintiffs, these
18 allegations are sufficient for the Court to conclude that the Carrier IQ Software undermines
19 consumers' reasonable expectations in privacy to such a degree so as to render their mobile devices
20 unfit to perform their core functions. During discovery, the parties will have the opportunity to flesh
21 out the precise way the Carrier IQ Software operates, including the degree to which Plaintiffs'
22 personal data or communications were in fact compromised by the Carrier IQ Software. Based on
23 development of a factual record, Carrier IQ Software may renew their argument via motion for
24 summary judgment.

25 ///

26 ///

27 ///

28 ///

Accordingly, for the foregoing reasons, Plaintiffs have adequately alleged that their mobile devices were unmerchantable and Defendants motion to dismiss the implied warranty claims on this ground is **DENIED**.¹³

F. Plaintiffs' Magnuson-Moss Warranty Act Claims Necessarily Depend on the State Law Implied Warranty Claims

The Magnuson-Moss Warranty Act “does not create implied warranties, but instead confers federal court jurisdiction for state law breach of implied warranty claims.” *IWOI, LLC v. Monaco Coach Corp.*, 581 F. Supp. 2d 994, 999 (N.D. Ill. 2008). Thus, while the Act “creates a separate federal cause of action for breach of an implied warranty, courts must look to state law to determine the meaning and scope of the implied warranty.” *MacDonald v. Ford Motor Company*, — F. Supp. 2d —, 2014 WL 1340339, at *12 (N.D. Cal. Mar. 31, 2014). Accordingly, Plaintiff’s Magnuson-Moss claims “hinge on the state law warranty claims.” *See Clemens*, 534 F.3d at 1022 n.3 (“Therefore, the federal claims hinge on the state law warranty claims.”). As detailed above, the Court has declined to dismiss all of Plaintiffs’ state implied warranty claims at this stage. Accordingly, Defendant’s motion to dismiss Plaintiffs’ Magnuson-Moss Warranty Act Claims is **DENIED**.

G. State Consumer Protection Statutes

Defendants have moved to dismiss Plaintiffs’ state consumer protection statute-based claims. The bulk of Defendants’ arguments are directed to the California UCL claim, with similar arguments being made as to the various other states’ laws.

///

///

¹³ Plaintiffs argue that the Carrier IQ Software also renders their mobile devices unmerchantable because it depletes battery power and life, thus reducing the lifespan of their mobile device battery. The Court rejects this argument. There are no allegations that would permit the inference that the Carrier IQ Software’s impact on a mobile device’s battery is so significant as to render the device unfit for its ordinary purpose. *See Tomek v. Apple, Inc.*, 2:11-cv-02700-MCE-DAD, 2012 WL 2857035 (E.D. Cal. July 11, 2012) (“Plaintiff’s allegations that, under unique circumstances, namely ‘heavy loads’ undertaken when the battery is already low, the MacBook may shut down, and that his computer shut down once over the course of a six month period, are insufficient as a matter of law to state a claim that the MacBook is not fit for ordinary use.”).

1. California Unfair Competition Law Claims, Cal. Bus. & Prof. Code § 17200

Plaintiffs allege that Defendants' conduct regarding the Carrier IQ Software constitutes unfair, unlawful, and fraudulent conduct in violation of the California UCL. Defendants move to dismiss Plaintiffs' prong under all three of the prongs.

a. Plaintiffs' Have Stated a Claim for Violation of the UCL Fraud-Prong Based on Defendants' Alleged Omissions

To state a claim under the "fraudulent" prong of the UCL, "it is necessary only to show that members of the public are likely to be deceived" by the business practice. *In re Tobacco II Cases*, 46 Cal.4th 298, 312 (2009). Following the passage of Proposition 64, the California Supreme Court has held that a plaintiff stating a claim under the "fraud" prong must plead actual reliance. *See id.* at 326 (interpreting Proposition 64 as "impos[ing] an actual reliance requirement on plaintiffs prosecuting a private enforcement action under the UCL's fraud prong"); *see also Morgan v. AT&T Wireless Servs., Inc.*, 177 Cal. App. 4th 1235, 1257 (2009) ("In *Tobacco II*, the Supreme Court held that this standing requirement . . . imposes an actual reliance requirement on named plaintiffs seeking relief under the fraudulent prong of the UCL." (citation omitted)); *Rosado v. eBay*, — F. Supp. 2d —, 2014 WL 2945774, at *5 (N.D. Cal. June 30, 2014) (noting that *Tobacco II* held "that for a fraudulent business practices claim, the UCL mandates that plaintiff demonstrate 'actual reliance' upon the defendant's misrepresentation or omission").

Claims under the UCL fraudulent prong must meet the heightened pleading standard of Federal Rule of Civil Procedure 9(b). *See, e.g., Grant v. Pensco Trust Co., LLC*, No. 12-cv-06084-WHO, 2014 WL 1471054, at *6 (N.D. Cal. Apr. 15, 2014).

In the SCAC, Plaintiffs contend that the Defendants engaged in fraudulent conduct by failing to disclose the existence and functionality of the Carrier IQ Software. Specifically, they allege:

Defendants secretly installed the Carrier IQ Software on plaintiffs' . . . mobile devices; failed to disclose that the Carrier IQ Software was always operating on such devices; failed to disclose that the carrier IQ Software was capable of intercepting private communications, and that it in fact did intercept such communications; and failed to disclose that the Carrier IQ Software degraded the performance of their devices by overtaxing processor power and device memory, and by depleting battery power and life.

SCAC ¶ 120. Plaintiffs allege that Defendants had a duty to “disclose the presence and functionality of the Carrier IQ Software” because “only defendants knew of the installation and functionality of the Carrier IQ Software” and “knew that the existence of the Carrier IQ Software was not known or reasonably discoverable by plaintiffs and the class.” *Id.* ¶ 122.

Omissions can form the basis of a fraudulent prong UCL claim. “For an omission to be actionable under the UCL, ‘the omission must be contrary to a representation actually made by the defendant, or an omission of a fact the defendant was obliged to disclose.’” *In re Adobe Systems, Inc. Privacy Litig.*, — F. Supp. 2d —, C13-05226 LHK, 2014 WL 4379916, at *20 (N.D. Cal. Sept. 4, 2014) (quoting *Daugherty v. Am. Honda Motor Co.*, 144 Cal. App. 4th 824, 835 (2006)) (emphasis added). A defendant has a “duty to disclose” information in one of four instances: (1) when the defendant is the plaintiff’s fiduciary; (2) when the defendant has exclusive knowledge of material facts not known or reasonably accessible to the plaintiff; (3) when the defendant actively conceals a material fact from the plaintiff; or (4) when the defendant makes partial representations that are misleading because some other material fact has not been disclosed. *Id.*; see also *Collins v. eMachines, Inc.*, 202 Cal. App. 4th 249, 255 (2011) (same). “A non-disclosed fact is material ‘if the omitted information would cause a reasonable consumer to behave differently if he or she was aware of it.’” *Elias*, 2014 WL 493034, at *6 (quoting *O’Shea v. Epson Am., Inc.*, No. 09-8063, 2011 WL 3299936 (C.D. Cal. July 29, 2011)); see also *Ehrlich v. BMW of N. Am, LLC*, 801 F. Supp. 2d 908, 916 (C.D. Cal. 2010) (“In an omissions case, omitted information is material if a plaintiff can allege that, ‘had the omitted information been disclosed, one would have been aware of it and behaved differently.’ Materiality is viewed from the prospective of the reasonable consumer.” (citation omitted)).

Defendants argue that the Court should dismiss the fraudulent prong claim because Plaintiffs have failed to comply with Rule 9(b). In *Marolda v. Symantec Corp.*, 672 F. Supp. 2d 992 (ND. Cal. 2009), Judge Patel stated that in order to comply with Rule 9(b) in an omission-based fraud action, plaintiffs had to

describe the content of the omission and where the omitted information should or could have been revealed, as well as provide representative samples of advertisements, offers, or other

representations that plaintiff[s] relied on to make [their] purchase[s] and that failed to include the allegedly omitted information.

Id. at 1002. “Subsequent cases have, however, called into question these specific requirements spawned by the *Marolda* court” and the “requirements are not necessarily appropriate for all cases alleging a fraudulent omission.” *Overton v. Bird Brain, Inc.*, No. SACV 11-1054 DOC (ANx), 2012 WL 909295, at *5-6 (C.D. Cal. Mar. 15, 2012).

For example, in *MacDonald v. Ford Motor Co.*, — F. Supp. 2d —, 2014 WL 1340339 (N.D. Cal. Mar. 31, 2014), the court noted that *Marolda* involved a complaint with dissimilar factual allegations. It recognized that *Marolda* “concerned an alleged omission within a particular advertisement, which the plaintiff had failed to produce or adequately describe.” *Id.* at *6. Thus, in *Marolda*, the ““ content of the representation [was] clearly within plaintiff’s knowledge.” *Id.* (quoting *Marolda*, 672 F. Supp. 2d at 1001). After recognizing that courts had held that the *Marolda* requirements were not “necessarily appropriate” for all omissions cases, the court in *MacDonald* stated:

Typically, “[a]verments of fraud must be accompanied by the who what when where, and how of the misconduct charged,” but claims based on an omission “can succeed without the same level of specificity required by a normal fraud claim.” This is because a plaintiff alleging an omission-based fraud will “not be able to specify the time, place, and specific content of an omission as would a plaintiff in a false representation claim.” Because the plaintiffs “[are] alleging a failure to act instead of an affirmative act, the [Plaintiffs] cannot point out the specific moment when the Defendant failed to act.”

Id. at *6 (quoting first *Cooper v. Pickett*, 137 F.3d 616, 627 (9th Cir. 1997), and then *Baggett v. Hewlett-Packard Co.*, 582 F. Supp. 2d 1261, 1267 (C.D. Cal. 2007)).

Here, Plaintiffs have clearly alleged the content of the alleged omission – the installation and functionality of the Carrier IQ Software. SCAC ¶ 120. Further, it appears they have alleged materiality by alleging that had they been aware of the installation and functionality of the Carrier IQ Software, they would not have purchased their mobile devices. *Id.* ¶ 3 (“[P]laintiffs and members of the proposed class have suffered economic harm; they would not have purchased their mobile devices had they known that these devices bore hidden battery-, processor- and memory-taxing

software that intercepts private and confidential communications that enables them to be sent to unintended recipients.”); *id.* ¶ 74 (“Mobile device owners were unaware of this functionality of their Carrier IQ Software-bearing devices, and it is one more reason why they would not have purchased these devices had they known they were bearing the Carrier IQ Software that operated in the manners alleged). Finally, Plaintiffs have alleged that the information regarding the Carrier IQ Software was in the exclusive knowledge of Defendants. *Id.* ¶ 122. These allegations are sufficient to plausibly allege that Defendants had exclusive knowledge of a material fact that they had a duty to disclose but chose to omit.

Nonetheless, Defendants contend that courts in omission cases have required plaintiffs to allege that *had* a material fact been disclosed, the plaintiffs *would have* been aware of the disclosure. Defendants contend this is part of the “actual reliance” requirement under the UCL. In *Hoffman v. 162 North Wolfe LLC*, 228 Cal. App. 4th 1178 (2014), the California Court of Appeal held that “[r]eliance can be proved in a fraudulent omission case by establishing that had the omitted information been disclosed, [the plaintiff] would have been aware of it and behaved differently.” *Id.* at 1193-94 (quoting *Boschma v. Home Loan Center, Inc.*, 198 Cal. App. 4th 230, 250 (2011)). Thus, in *Ehrlich*, the district court found that plaintiff had alleged that BMW omitted a material fact – a defect in BMW windshields making them prone to cracking. However, the court dismissed the omission claim with leave to amend, finding that plaintiff had failed to allege that had the defect been disclosed, he would have been aware of it

Given the importance of the cracking defect, had BMW chosen to disclose it to prospective buyers, presumably Plaintiff, as a member of the buying public, would have become aware of the defect in the course of making his purchasing decision. Nevertheless, the Court agrees with BMW that the FAC is devoid of allegations that Plaintiff would have plausibly been aware of the cracking defect before he purchased his MINI and BMW publicized this information.

Ehrlich, 801 F. Supp. 2d at 920; *see also In re Facebook Advertising Litig.*, No. 5:09-cv-03043, 2010 WL 3341062, at *10 (N.D. Cal. Aug. 25, 2010) (stating in the reliance context that “Plaintiffs still should be able to identify with particularity at least the specific policies and representations that they reviewed”).

While a close issue, the Court finds that the SCAC contains sufficient allegations from which it can be inferred that had Defendants reasonably disclosed the existence and functionality of the Carrier IQ Software – a material fact exclusively in Defendants’ knowledge – Plaintiffs would have been aware of it. First, as detailed above, Plaintiffs have alleged that had they been aware of the Carrier IQ Software, they would not have purchased affected mobile devices. *See, e.g., In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 988 (S.D. Cal. 2014) (“[B]ecause Plaintiffs have alleged that Sony omitted material information regarding the security of Sony Online Services, and that this information should have been disclosed to consumers at the time consumers purchased their Consoles, the Court finds Plaintiffs have sufficiently alleged a loss of money or property ‘as a result’ of Sony’s alleged unfair business practices.”); *Elias*, 2014 WL 493034, at *6 (“Plaintiff has adequately pleaded materiality by alleging that he would have acted differently by not purchasing the computer as ordered had he known about the insufficiency of the included PSU.”). Second, the SCAC contains extensive allegations regarding the public outcry regarding the Carrier IQ Software once its existence became public knowledge – including media reports and Senator Franken sending letters of inquiry to mobile carriers. The intensity of their outcry underscores the materiality of the alleged omission.

In light of the SCAC’s allegations, the Court finds there is a sufficient basis to plausibly conclude that had Defendants disclosed the existence and functionality of the Carrier IQ Software, Plaintiffs would have been aware of it and acted differently. Defendants remain free, however, to explore Plaintiffs’ reliance during discovery and, if necessary, re-raise this argument during class certification or summary judgment.

b. Plaintiffs Have Adequately Plead a Violation of the Unfairness Prong of the UCL

Under the unfairness prong of the UCL, “‘a practice may be deemed unfair even if not specifically proscribed by some other law.’” *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1143 (2003) (quoting *Cel-Tech Commc’ns, Inc. v. Los Angeles Cellular Telephone Co.*, 20 Cal. 4th 163, 180 (1999)). The term “unfair” is undefined in the statute and the Ninth Circuit has noted that the “proper definition of ‘unfair’ conduct against consumers ‘is currently in flux’ among

California courts.” *Davis v. HSBC Bank Nevada, NA*, 691 F.3d 1152, 1169 (9th Cir. 2012). In *Drum v. San Fernando Valley Bar Ass’n*, 182 Cal. App. 4th 247 (2010), the California Court of Appeal articulated three possible tests defining “unfair.” First, the “tethering test” requires that the “public policy which is a predicate to a consumer unfair competition action under the ‘unfair’ prong of the UCL must be tethered to specific constitutional, statutory, or regulatory provisions.” *Id.* at 257 (quoting *Bardin v. Daimlerchrysler Corp.*, 136 Cal. App. 4th 1273-74 (2006)). The second test, which has been referred to as the “balancing test”, asks whether the alleged business practice is “immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers and requires the court to weigh the utility of the defendant’s conduct against the gravity of the harm to the alleged victim.” *Id.* (quoting *Bardin*, 136 Cal. App. 4th at 1260). Finally, the third test incorporates the definition of “unfair” from the Federal Trade Commission Act and requires: (1) that the consumer injury be substantial; (2) that the injury not be outweighed by any countervailing benefits to consumers or competition; and (3) the injury is one that consumers could not have reasonably avoided. *Id.*

Plaintiffs’ SCAC contains allegations relating to both the “tethering” and “balancing” tests. It alleges:

Defendants’ conduct lacks reasonable and legitimate justification in that defendants have benefitted from such conduct and practices while plaintiffs and prospective class members have been misled as to the nature and integrity of defendants’ goods and services and have, in fact, suffered injury regarding the privacy and confidentiality of their personal information and the use of their device resources. Further, defendants’ conduct is unfair because it offends California public policy as reflected in the right to privacy enshrined in the state constitution; California Penal Code §§ 502, 631, and 632.7; and California statutes recognizing the need for consumers to safeguard their privacy interests, including California Civil Code § 1798.80.

SCAC ¶ 119.

As to the “tethering” test, Defendants argue that Plaintiffs’ allegations that their conduct has offended California public policy fail because Plaintiffs have not plead sufficient facts that Defendants’ conduct violated California Penal Code §§ 502, 631, 632.7, Cal. Civil Code § 1798.80, or the California Constitution. *See also In re Google, Inc. Privacy Policy Litigation*, — F. Supp. 2d —, 2014 WL 3707508, at *10 (N.D. Cal. July 21, 2014) (dismissing unfairness prong

claim because plaintiffs had failed to allege facts sufficient to “[p]rove a claim under the California Constitutional right to privacy”); *Tat Tohumculuk, A.S. v. H.J. Heinz Company*, No. Civ. 13-0773 WBS KJN, 2013 WL 6070483 (E.D. Cal. Nov. 14, 2013) (“To the extent plaintiff tethers its unfairness claims to § 1981 and section 51, the claims fails for the same reasons set forth above. Accordingly, because plaintiff does not successfully allege a violation of any underlying statutory provision, the court will grant defendants’ motion to dismiss plaintiff’s UCL claim.”). Accordingly, there is case law which suggests that the failure to actually allege a violation of a specific statute or constitutional provision will foreclose result under the “tethering” unfairness prong test.

The Court concludes, however, that these cases have read the “tethering test” too narrowly and essentially conflates the “unfair” and “unlawful” prongs under the UCL. As already stated, an act can be “unfair” even if not unlawful. *See In re Adobe Systems*, 2014 WL 4379916, at *17. Additionally, the “tethering” test merely requires that the *public policy* that has allegedly been offended be tied to a specific statutory provision. As Judge Koh has recognized,

Turning to the “tethering test,” the Court notes that contrary to Adobe’s assertion, Plaintiffs do not need to plead any direct violations of a statute to bring a claim under the UCL’s unfair prong. Instead, Plaintiffs need merely to show *that the effects of Adobe’s conduct “are comparable to or the same as a violation of the law, or otherwise significantly threaten[] or harm [] competition.”*

Id. at *18 (quoting *Cal-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.*, 20 Cal. 4th 163, 185 (1999)) (emphasis added). In that case, plaintiffs had alleged that Adobe employed “deeply flawed” security practices that failed to conform to industry standards and contributed to hackers accessing Adobe’s customers’ personal information. *Id.* at *2. Plaintiffs contended that Adobes actions violated California’s public policy of “protecting customer data,” allegedly embodied in three statutes. *Id.* at 18; *see also, e.g.*, Cal. Civ. Code § 1798.1 (“The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them”); Cal. Civ. Code § 1798.81.5(a) (“It is the intent of the Legislature to ensure that personal information about California residents is protected.”). Judge Koh found that “California legislative intent is clear on this point,” and thus found that “Plaintiffs ha[d] adequately alleged that Adobe’s conduct [was] ‘comparable’ to a violation of law.” *In re Adobe*, 2014 WL 4379916, at *18; *see also Jolley v.*

1 *Chase Home Finance*, 213 Cal. App. 4th 872, 907-08 (2013) (reversing summary judgment on
 2 unfairness UCL claim based on alleged “dual tracking” of mortgages because, while not illegal at
 3 the time of defendant’s conduct, “the new legislation [regarding dual tracking] and its legislative
 4 history may still contribute to its being considered ‘unfair’ for purposes of the UCL”).

5 Likewise, in *Boris v. Wal-Mart Stores, Inc.* — F. Supp. 2d — , 2014 WL 1477404 (C.D. Cal.
 6 Apr. 9, 2014), the district court dismissed plaintiff’s unfairness-prong UCL claim under the tethering
 7 test. This claim was dismissed, however, not because of Plaintiffs’ failure to sufficiently allege that
 8 defendants’ conduct violated a statute or constitutional provision, but because “[p]laintiffs have not
 9 pointed to any specific constitutional, statutory, or regulatory provision that *embodies a policy that*
 10 *Equate Migraine’s price and red packaging violate.*” *Id.* at *6 (emphasis added). Similarly, in
 11 *Graham v. Bank of America, N.A.*, 226 Cal. App. 4th 594 (2014), the California Court of Appeal
 12 affirmed dismissal of an “unfairness” prong UCL claim based on defendant’s “highly speculative
 13 appraisal methods” used to support “unnecessarily large variable rate loan packages” which
 14 allegedly misled consumers. *Id.* at 611. The court found that plaintiff had failed to “allege any
 15 statements about the appraisal or opinions about the possible future value of the home constitute
 16 conduct tethered to a violation of a constitutional, statutory, or regulatory provision.” *Id.* at 613.

17 Plaintiffs have sufficiently identified a California public policy in ensuring that private
 18 communications or data are not intercepted, *see, e.g.*, Cal. Penal Code §§ 502 (making illegal
 19 unauthorized access to computers, computer systems, or computer data), 631 (making illegal for an
 20 individual to, without consent, “read[], attempt[] to read, or to learn the contents or meaning of any
 21 message, report, or communication while the same is in transit”), or privacy in general, *see* Cal.
 22 Const. art. 1, § 1 (“All people are by nature free and independent and have inalienable rights.
 23 Among these are enjoying and defending life and liberty, acquiring, possession, and protecting
 24 property, and pursuing and obtaining safety, happiness, and privacy.”); *see also Pioneer Electronics*
 25 *(USA), Inc. v. Superior Court*, 40 Cal. 4th 360, 370 (2007) (“[T]he right of privacy [under the
 26 California Constitution] protects the individual’s *reasonable* expectation of privacy against a serious
 27 *invasion...*”). The SCAC – alleging in detail, as detailed above, that the Carrier IQ Software
 28

surreptitiously intercepts various personal information – sufficiently alleges for purposes of the pleading stage that Defendants’ conduct offended the public policy reflected in these provisions.

Further, Plaintiffs have stated a claim under the UCL-unfairness “balancing” test. Plaintiffs have adequately alleged conduct (interception and transmission of private and confidential communications and data) that plausibly could outweigh the utility of such conduct to Defendants. The cost-benefit analysis this test calls for is not properly suited for resolution at the pleading stage. For example, in *In re iPhone Application Litigation*, 844 F. Supp. 2d 1040 (N.D. Cal. 2012), the court held:

Plaintiffs have alleged . . . Apple makes affirmative representations regarding its protection of user’s personal information. In contrast, according to Plaintiffs, Apple allowed third parties to collect consumers’ information without their knowledge. While the benefits of Apple’s conduct may ultimately outweigh the harm to consumers, this is a factual determination that cannot be made at this stage of proceedings. Nor can the Court conclude at this stage that Apple’s practices are not injurious to consumers as a matter of law.

Id. at 1073.

Accordingly, for the foregoing reasons, Defendants’ motion to dismiss Plaintiff’s California UCL-unfairness prong claim is **DENIED**.

c. Plaintiffs’ Unlawful Prong Claim Will Be Dismissed With Leave to Amend

Plaintiffs base their UCL “unlawful” prong claims on alleged violations of the Federal Wiretap Act, Cal. Penal Code §§ 502, 631, and 632.7, and the fact that HTC violated the Federal Trade Commission Act. SCAC ¶ 118. The Court has previously dismissed Plaintiff’s Cal. Penal Code § 502 and Wiretap Act causes of action with leave to amend. The Court defers ruling on Plaintiffs’ unlawful prong UCL claim pending Plaintiffs’ amendment to attempt to successfully assert a Wiretap Act or Cal. Penal Code § 502 claim.

2. Connecticut Unlawful Trade Practices Act, Conn. Gen. Stat. § 42-110a

The Connecticut Unlawful Trade Practices Act (“CUTPA”) generally prohibits individuals from “engag[ing] in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce.” Conn. Gen. Stat. § 42-110b(a). “A claim under CUTPA requires that [the] plaintiff allege that [the] defendant engaged in unfair methods of competition and

unfair or deceptive acts or practices in the conduct of any trade or commerce.” *Star Child II, LLC v. Lanmar Aviation, Inc.*, No. 3:11-CV-01842(AWT), 2013 WL 1103915 (D. Conn. Mar. 16, 2013).

The Connecticut Supreme Court has adopted the following factors for determining whether a trade practice is “unfair or deceptive”:

(1) Whether the practice, without necessarily having been considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise – whether, in other words, it is within at least a penumbra of some common law, statutory, or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; and (3) whether it causes substantial injury to consumers, competitors, or other businessmen.

Harris v. Bradley Memorial Hosp. & Health Center, Inc., 994 A.2d 153, 173 (Conn. 2010).

Defendants contend that Plaintiffs’ CUTPA claim should be dismissed because Defendants did not have “any duty in the first instance to disclose the presence or functionality of the Carrier IQ software” and therefore have not alleged any “unfair or deceptive acts or practices” for purposes of CUTPA. Docket No. 304, at 60.

The Connecticut courts have held that when a plaintiff “alleges that a defendant’s *passive* conduct violates CUTPA . . . common sense dictates that a court should inquire whether the defendant was under any obligation to do what it refrained from doing.” *DiTeresi v. Stamford Health Sys., Inc.*, 63 A.3d 1011, 1023 (Conn. Ct. App. 2013). Accordingly, where a CUTPA claim is based on a failure to disclose information, Connecticut courts first look to whether the defendant had a duty to disclose the information in question. *See, e.g., Kenney v. Healey Ford-Lincoln-Mercury, Inc.*, 730 A.2d 115, 117 (Conn. Ct. App. 1999) (“A failure to disclose can be deceptive only if, in light of all the circumstances, there is a duty to disclose.”). “Regarding the duty to disclose, the general rule is that . . . silence . . . cannot give rise to an action” however, “[a] duty to disclose will be imposed . . . on a party insofar as he voluntarily makes disclosure. A party who assumes to speak must make a full and fair disclosure as to the matters about which he assumes to speak.” *Miller v. Guimaraes*, 829 A.2d 422, 434-35 (Conn. Ct. App. 2003).

Defendants rely primarily on *Putnam Bank v. Ikon Office Solutions, Inc.*, No. 3:10-cv-1067, 2011 WL 2633658 (D. Conn. July 5, 2011) for its assertion that Defendants did not have a duty to disclose the presence and functionality of the Carrier IQ Software on the mobile devices. In *Putnam*

1 Bank, plaintiff alleged that the defendant, Ikon, knew that copiers and fax machines it sold and
 2 leased contained “automatic storage devices” that saved images of documents that had been faxed,
 3 printed, or scanned and that Ikon did not destroy the saved images before it sold or leased the
 4 equipment to another person. *Id.* at *1. Plaintiffs alleged that Ikon failed to disclose this fact. The
 5 court dismissed plaintiffs’ CUTPA claim finding that Ikon had no duty to disclose the presence of
 6 the automatic storage devices. It stated:

7 the essence of the transactions between Putnam and Ikon was the lease
 8 of office equipment, not the protection of data that would be saved on
 9 the equipment. Putnam does not allege that Ikon knew about
 10 Putnam’s apparent lack of familiarity with digital storage devices or
 11 that Ikon knew there was a custom or other objective circumstance that
 would cause Putnam to believe that data security would be covered by
 the leases. Ikon therefore could not have known that Putnam may
 have entered into the leases on the incorrect assumption that data
 security did not need to be mentioned explicitly in the leases.

12 *Id.* at *3. Defendants here argue that the essence of the transaction between Plaintiff McKeen and
 13 Defendants was the sale of a phone, not the handling of the data that would be saved on that phone.
 14 Docket No. 304, at 61.

15 The Court has located no Connecticut case that imposes a broad duty to disclose on
 16 defendants (or one commensurate with California’s UCL). *Cf. Glazer v. Dress Barn, Inc.*, 873 A.2d
 17 929, 961 (Conn. 2005) (noting that a duty to disclose can arise where a party makes a voluntary
 18 disclosure, where it is imposed by statute or regulation, or where a special relationship gives rise to a
 19 fiduciary duty). As currently pled, the SCAC fails to plead facts from which a duty to disclose
 20 information can be inferred. Accordingly, Plaintiffs CUTPA claim will be **DISMISSED** with leave
 21 to amend so that Plaintiffs may attempt to allege sufficient facts demonstrating that Defendants’ had
 22 a duty to disclose the presence and functionality of the Carrier IQ Software. Notably, Plaintiffs have
 23 cited no case in Connecticut that applies a broad duty to disclose like California.

24 3. Florida Deceptive & Unfair Trade Practices Act, Fla. Stat. § 501.201

25 A claim for damages under the Florida Deceptive & Unfair Trade Practices Act
 26 (“FDUTPA”) has three elements: (1) a deceptive act or unfair practice; (2) causation; and (3) actual
 27 damages. *See Garcia v. Kashi Co.*, — F. Supp. 2d —, 2014 WL 4392163, at *16 (S.D. Fla. Sept. 5,
 28 2014). An “unfair practice is ‘one that offends established public policy and one that is immoral,

1 unethical, oppressive, unscrupulous or substantially injurious to consumers.” *PNR, Inc. v. Beacon*
 2 *Property Mgmt., Inc.*, 842 So.2d 773, 777 (Fla. 2003). “Deception occurs if there is a
 3 representation, omission, or practice that is likely to mislead consumers acting reasonably in the
 4 circumstances, to the consumers’ detriment.” *State v. Beach Blvd. Automotive Inc.*, 139 So.3d 380,
 5 387 (Fla. Ct. App. 2014).

6 Defendants argue that where an alleged deceptive act is a failure to disclose information, the
 7 plaintiff must establish that a duty to disclose actually exists. They cite *Virgilio v. Ryland Grp., Inc.*,
 8 680 F.3d 1329 (11th Cir. 2012), for this proposition, but this case does not support their position.
 9 All the Eleventh Circuit did in that case was affirm dismissal of a FDUTPA claim because the only
 10 predicate act plaintiff alleged was a breach of an “affirmative duty of disclosure” in the context of a
 11 real estate transaction. Earlier in the opinion, the court had determined that there was no affirmative
 12 duty of disclosure in that context under Florida law. *Id.* at 1338. Contrary to Defendants’ assertion,
 13 at least one court in Florida has held that a “duty to disclose is not an element of FDUTPA.” *Morris*
 14 *v. ADT Sec Services*, 580 F. Supp. 2d 1305, 1310 (S.D. Fla. 2008). In *Morris*, the court found
 15 plaintiff had stated an omission-based FDUTPA claim based on the allegation that ADT sold a
 16 security system that it knew would stop working after 5 years “without disclosing this fact to
 17 customers” and then charged customers to upgrade the system to work as originally promised. *Id.*

18 Defendants further argue that Plaintiffs have failed to demonstrate “actual damages” as the
 19 result of the Carrier IQ Software. “Actual damages” are defined by the FDUTPA as “the difference
 20 in the market value of the product or service in the condition in which it was delivered and the
 21 market value in the condition in which it should have been delivered according to the contract of the
 22 parties.” *Rollins, Inc. v. Heller*, 454 So.2d 580 585 (Fla. Ct. App. 1984). However, under
 23 “FDUTPA, Plaintiffs suffered damages when they purchased something that was not what they were
 24 led to believe they were purchasing.” *Point Blank Solutions, Inc. v. Toyobo Am., Inc.*, No. 09-
 25 61166-CIV, 2011 WL 1833366, at *6 (S.D. Fla. May 13, 2011).

26 Under this “market value” theory, Plaintiffs have sufficiently alleged actual damages.
 27 Plaintiffs have alleged that they suffered ascertainable loss as a result of them overpaying for their
 28 mobile devices (or their mobile devices losing value) because their resources were being taxed by

the constantly running Carrier IQ Software (as well as the privacy issues inherent in having the software on the mobile devices). SCAC ¶ 147. Plaintiffs allege that they and the class overpaid for the mobile devices and did not receive the benefit of the bargain. The value of their mobile device have diminished now that the privacy issues have come to light, and plaintiffs and the class purchased mobile devices that are not secure and private. *See, e.g.*, SCAC ¶¶ 147, 156, 164, 182, 201, 207, 218. These allegations are plausible – if, as is alleged, the Carrier IQ Software intercepts and transmits personal information and has a noticeable impact on the mobile device’s resources, the device plausibly is not as valuable on the market as one that does not have the software. Accordingly, for purposes of the pleading stage, the Court finds damages adequately alleged under FDUTPA.

For the foregoing reasons, Defendants’ motion to dismiss Plaintiffs’ FDUTPA claim is **DENIED**.

4. Maryland Consumer Protection Act, Md. Code. Com. L. § 13-101

Maryland’s Consumer Protection Act (“MCPA”) is materially similar to the statutes discussed above. The MCPA expressly provides that the “[f]ailure to state a material fact” is an unfair or deceptive trade practice “if the failure deceives or intends to deceive.” Md. Code Com. Law § 13-301(3). “Omissions are material under the MCPA ‘if a significant number of unsophisticated consumers would find that information important in determining a course of action.’” *Castle v. Capital One, N.A.*, No. WMN-13-1830, 2014 WL 176790, at *7 (D.Md. Jan. 15, 2014) (quoting *Bank of America, N.A. v. Jill P. Mitchell Living Trust*, 822 F. Supp. 2d 505, 534 (D.Md. 2011)). Plaintiffs must also allege reliance, and a consumer “relies on a material omission under the MCPA where it is substantially likely that the consumer would not have made the choice in question had the commercial entity disclosed the omitted information.” *Id.*

Defendants have moved to dismiss Plaintiffs’ MCPA claim on similar grounds discussed above, namely that Plaintiffs have failed to demonstrate that Defendants had a duty to disclose, have failed to show actual damages, and have failed to allege that they relied on any omission. The Court rejects the latter two arguments for the same reasons these arguments failed *supra*. As to the alleged duty to disclose, Maryland law expressly prohibits any person engaged in the “promotion or sale of

any consumer good[]” from engaging in an “omission of any material fact with the intent that a consumer rely on the same.” Md. Code Com. Law § 13-301(9)(i). This provision imposes on the sellers of consumer goods and services the duty to disclose all material facts. *See Doyle v. Chrysler Group LLC*, No. SACV 13-0620 JVS (ANx), 2014 WL 1910628, at *11. (C.D. Cal. Jan. 29, 2014) (holding that Maryland law imposes a legal duty to disclose material facts in consumer transactions). As discussed above in the context of the California UCL “unfairness” prong claim, Plaintiffs have sufficiently alleged that the existence and functionality of the Carrier IQ Software is “material.”

For the foregoing reasons, Defendants’ motion to dismiss Plaintiffs’ MCPA claim is **DENIED**.

5. Michigan Consumer Protection Act, Mich. Comp. Laws § 445.901

Defendants argue that Plaintiffs have failed to allege any basis for imposing a duty to disclose under the Michigan Consumer Protection Act. The Michigan Consumer Protection Act includes a proscription on “[f]ailing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer.” Mich. Comp. Law § 445.901(1)(s). This language imposes an affirmative duty on defendants to disclose a material fact when that fact is in the exclusive knowledge of the defendant. This test is materially similar to California law which, as discussed *supra*, imposes a duty to disclose material facts in similar circumstances. *See In re Porsche Cars North America, Inc.*, 880 F. Supp. 2d 801, 855 (S.D. Ohio 2012) (“This language [in Mich. Comp. Law § 445.903(1)(s)] mirrors the test that California courts employ in interpreting California’s consumer protection statute.”).

For the foregoing reasons Defendants’ motion to dismiss Plaintiffs’ Michigan Consumer Protection Act claim is **DENIED**.

6. Texas Deceptive Trade Practices Act, Tex. Bus. & Prof. Code § 17.41

To state a claim under the Texas Deceptive Trade Practices Act (“DTPA”), plaintiffs must allege that (1) they were consumers of Defendants’ goods or services; (2) Defendants violated a specific provision of the DTPA, and that Defendants acts were a “producing cause” of actual damages. *Amstadt v. U.S. Brass Corp.*, 919 S.W.2d 644, 649 (Tex. 1996). The DTPA proscribes four categories of conduct: (1) false, misleading, or deceptive acts or practices; (2) any

unconscionable action or course of action; (3) breach of an express or implied warranty; and (4) an act or practice in violation of Tex. Ins. Code § 541. *See* Tex. Bus. & Com. Code Ann. § 17.50(a). In the SCAC, Plaintiffs contend that Defendants violated the first three provisions. Defendants seek to dismiss each of Plaintiffs' claims.

a. Plaintiffs Have Adequately Alleged that Defendants Violated Specific Provisions of the DTPA

Defendants contend that Plaintiffs have failed to adequately allege that Defendants violated a specific provision of the DTPA. The DTPA defines "false, misleading, or deceptive acts or practices" to include "failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed." Tex. Bus. & Prof. Code § 17.46(b)(24). Defendants simply incorporate the arguments they raised against Plaintiffs' California UCL claims on this point, stating that "Plaintiffs have failed to plead any 'false, misleading, or deceptive' act with the particularity required by Rule 9(b)." Docket No. 304, at 67. Because Defendants have raised no specific argument as to the DTPA and the Court has previously rejected these arguments in the context of Plaintiffs' California UCL claim, the Court declines to dismiss Plaintiffs DTPA claim on this ground. Plaintiffs allege the failure to disclose the function and effect of the Carrier IQ Software was intended to and did induce consumers to purchase the subject phones.

Because Plaintiffs have adequately alleged at least one predicate violation of the DTPA, the Court need not address whether Plaintiffs have adequately stated a violation of any other DTPA provision.

b. Plaintiffs Have Failed to Allege that Defendants' Conduct Was a "Producing Cause" of Their Damages

Defendants first argue that any omission by them regarding the presence or functionality of the Carrier IQ Software was not a "producing cause" of any actual damages because the mobile carriers were capable of "assessing the suitability of the software's functionality for use in the mobile devices" they subsequently sold to Plaintiffs. Docket No. 304, at 67.

1 In *Ford Motor Co. v. Ledesma*, 242 S.W.3d 32 (Tex. 2007), the Texas Supreme Court
2 provided the following definition for “producing cause”:

3 Defining producing cause as being a substantial factor in bringing
4 about an injury, and without which the injury would not have
5 occurred, is easily understood and conveys the essential components
6 of producing cause that (1) the cause must be a substantial cause of the
7 event in issue and (2) it must be a but-for cause, namely one without
8 which the event would not have occurred.

7 *Id.* at 46.

8 In arguing that any omission by Defendants could not be the “producing cause” of Plaintiffs’
9 injuries, Defendants rely on *Amstadt v. U.S. Brass Corp.*, 919 S.W.2d 644 (Tex. 1996). There,
10 plaintiffs were homeowners who sued under the DTPA the manufacturers who made their home’s
11 defective plumbing system, alleging that the manufacturers had misrepresented various aspects of
12 those systems. The defendants included the actual manufacturers of the plumbing system (U.S.
13 Brass) as well as the manufacturer of a plastic compound (Celcon) used in the system that allegedly
14 had failed (Celanese). The court found that any misrepresentations by these defendants were not
15 sufficiently connected to the plaintiffs’ injuries.

16 The court found that the Texas Legislature had not “intended the DTPA to reach upstream
17 manufacturers and suppliers when their misrepresentations are not communicated to the consumer.”
18 *Id.* at 649. Accordingly, it held that the “defendant’s deceptive conduct must occur in connection
19 with a consumer transaction.” *Id.* As to defendant Celanese (the manufacturer of the compound that
20 allegedly failed), the court stated:

21 Celanese promoted the use of Celcon in plumbing applications to U.S.
22 Brass and other manufacturers, and knew that U.S. Brass used Celcon
23 to make fittings for its plumbing systems. Celanese did not control
24 U.S. Brass’ selection of raw materials, did not design the parts or
25 tools, and did not instruct or train the homebuilders’ plumbers. . . .
26 Celanese’s marketing efforts were limited to promoting its material to
27 the manufacturers of the plumbing systems. It did not market the
28 systems to homebuilders or building code officials, or market the
finished homes to the consumers. The manufacturers of the plumbing
systems and the building code officials, and to a lesser degree the
homebuilders, were intermediaries capable of assessing the suitability
of Celcon for use in the systems.

1 *Id.* at 650-51. Similarly, as to U.S. Brass, the actual manufacturer of the entire plumbing system, the
2 court stated:

3 Although the conduct of U.S. Brass comes closer to being in
4 connection with the plaintiffs' purchase of their homes than the
5 conduct of Shell or Celanese, it also falls short of meeting the nexus
6 required for DTPA liability. U.S. Brass exercised significant control
7 over the design and installation of the plumbing systems, but as with
8 Shell and Celanese, U.S. Brass had no role in the sale of the homes to
the plaintiffs. As with Shell, U.S. Brass' marketing efforts were not
intended to, nor were they, incorporated into the marketing of the
homes to the plaintiffs. Finally, U.S. Brass' products were subject to
independent evaluation by building code officials, homebuilders, and
the plumbing contractors who installed the materials.

9 *Id.* at 652. Accordingly, because both defendants were removed from the actual consumer
10 transaction at issue, and their alleged misrepresentations had not reached the consumer, the plaintiffs
11 did not have a DTPA cause of action against those defendants. The court noted, "While our words
12 have varied, the concept has been consistent: the defendant's deceptive trade act or practice is not
13 actionable under the DTPA unless it was committed *in connection with* the plaintiff's transaction in
14 goods or services." *Id.* at 650.

15 As currently plead, Plaintiffs have failed to adequately allege that Defendants' were a
16 "producing cause" of their actual damages. Plaintiffs have failed to allege either that they purchased
17 their mobile devices directly from a Defendant (in which case the Defendant is not an "upstream
18 manufacturer or supplier") or that Defendants' marketing efforts reached them as consumers. *See,*
19 *e.g., PPG Indus., Inc. v. JMB/Houston Centers Partners Ltd. Ptnshp.*, 146 S.W.3d 79 (Tex. 2004)
20 ("Of course, if manufacturers make representations or warranties directly to consumers, the latter
21 may sue directly (despite the absence of privity) for breach of express warranty or violation of the
22 DTPA." (footnote omitted)). Accordingly, the Court will **DISMISS** Plaintiffs' DTPA claim with
23 leave to amend to afford Plaintiffs an opportunity to meet the "producing cause" test as articulated
24 by the Texas Supreme Court in *Amstadt*.

25 7. Washington Consumer Protection Act, Wash. Rev. Code § 19.86.010

26 The Washington Consumer Protection Act ("WCPA") provides a private cause of action for
27 "[a]ny person who is injured in his or her business or property" by "[u]nfair methods of competition
28 and unfair or deceptive acts or practices in the conduct of any trade or commerce." Wash. Rev.

Code 19.86.020; 19.86.090. The elements of a claim under the WCPA are “(1) an unfair or deceptive act or practice, (2) occurring in trade or commerce, (3) impacting the public interest, (4) causing injury to the plaintiffs’s business or property and (5) the injury is causally linked to the unfair or deceptive act.” *Frias v. Asset Foreclosures Services, Inc.*, 957 F. Supp. 2d 1264, 1270 (W.D. Wash. 2013).

Defendants contend that Plaintiffs have failed to adequately allege “injury to the plaintiff’s business or property” as required. They rely on the case of *Cousineau v. Microsoft Corp.*, 992 F. Supp. 2d 1116 (W.D. Wash. 2012). In that case, the district court granted defendant’s motion to dismiss plaintiff’s WCPA claim on the ground tha tplaintiffs had failed to adequately allege an injury. Plaintiffs had purchased Microsoft smart phones and, as to injury, alleged that Microsoft’s collection of geo-location data diminished the value of her phone. *Id.* at 1128 (“In support of her CPA claim, Cousineau argues first that Microsoft’s conduct diminished the value of her phone, and second that the unauthorized transmission of data ‘to its servers caused a diminution in users’ data plans.’”). The court found this was insufficient because plaintiff provided “no support for the assertion that the covert tracking diminished the phone’s market value.” *Id.*

Defendants’ argument on this point echoes their arguments made in challenging Plaintiffs’ Article III standing – arguments the Court has addressed *supra*. While Defendants’ arguments are not without force, the Court concludes they are premature at this stage. The Court determines it is plausible that, as currently alleged, the Carrier IQ Software would have a noticeable, not-insignificant impact on the market value of Plaintiffs’ mobile devices. This is entirely consistent with the *Cousineau* decision. It is one thing to have a mobile device that allegedly collects geolocation data. It is something quite different to have a device that compromises the user’s text messages, passwords, internet search terms, and the like by making them available for transmission to third parties. Further, to the extent the Carrier IQ Software operated continually in the background, it is plausible that its operating taxed the mobile devices resources and battery such that it had a noticeable impact on the performance (and thus the value) of the mobile phones. For purposes of the pleading stage, these allegations are sufficient to allege actionable damages.

Defendants remain free to challenge the factual and legal basis for these alleged damages after discovery at the summary judgment stage.

Defendants also argue that to the extent that Plaintiff Sandstrom's WCPA claim is based on HTC's failure to disclose the "deactivate debug code" error that permitted text messages from being copied into the system log and then transmitted to HTC, the claim should be dismissed because Plaintiffs do not allege that HTC was aware of this issue at the time of the transaction. The WCPA imposes a broad duty of disclosure on defendants – they have a "general duty . . . to disclose facts material to a transaction when the facts are *known to the seller* but not easily discoverable by the buyer." *Griffith v. Centex Real Estate Corp.*, 969 P.2d 486, 492 (Wash. Ct. App. 1998) (emphasis added). However, this duty to disclose requires that the seller *know* the facts that are at issue.

Defendants argue that the SCAC and FTC investigation reveal that HTC's conduct regarding the "debug code deactivation" was a mistake. The SCAC seems to suggest HTC did not knowingly engage in the transmission as it quotes extensively from an FTC investigation which speaks of HTC failing to deactivate the code and being unaware of that fact, and stating that "HTC could have detected its failure to deactivate the debug code in its CIQ Interface had it had adequate processes and tools in place for reviewing and testing the security of its software code." SCAC ¶ 77.

Plaintiffs do not respond to this latter argument by Defendants. Given the nature of the "debug deactivation" error as alleged in the SCAC and Plaintiffs' failure to respond, the Court concludes that Plaintiff Sandstrom's WCPA claim should be dismissed with prejudice to the extent it relies on HTC's alleged failure to disclose the "debug" error.

IV. CONCLUSION

For the foregoing reasons, the Court **GRANTS** in part and **DENIES** in part Defendants' motion to dismiss. Specifically, the Court dismisses the following claims with leave to amend:

- Plaintiffs' Wiretap Act claim is dismissed for failure to allege that the Device Manufacturers intentionally intercepted any communication as defined by the Wiretap Act.
- Plaintiffs' Cal. Penal Code § 502 claim is dismissed for failure to specify which specific provisions of this section Defendants are alleged to have violated.

- Plaintiffs' implied warranty claim arising under California law is dismissed for failure to allege facts in support of an exception to California's privity requirement. Further, Plaintiff's Song-Beverly Act claim is dismissed for failure to allege that any Plaintiff purchased a mobile device in California.
- Plaintiffs' Unfair Competition Law claim is dismissed to the extent it relies on allegedly "unlawful" conduct pending Plaintiffs adequately alleging a violation of the Wiretap Act or a California law or regulation.
- Plaintiffs' claim under the Connecticut Unlawful Trade Practices Act is dismissed for failure to allege that Defendants' had a duty to disclose the existence and operation of the Carrier IQ Software under Connecticut law.
- Plaintiffs' claim under the Texas Deceptive Trade Practices Act is dismissed for Plaintiffs' failure to allege Defendants' marketing efforts reached consumers or that their conduct was otherwise a "producing cause" of their injury as that phrase is interpreted by Texas courts.
- Plaintiffs' claim under the Washington Consumer Protection Act against HTC is dismissed to the extent it relies on HTC's failure to disclose the "debug" error.
- Plaintiffs' implied warranty claims under the laws of Maryland, Michigan, and Texas are dismissed without prejudice for failure to provide pre-suit notice to the Defendants.

The Court dismisses, with prejudice, Plaintiffs' claim under the Illinois Eavesdropping Law, 720 Ill. Comp. Stat. § 5/14-2(a)(1).

Finally, the Court dismisses, without prejudice, those state law claims arising under the laws of states in which no named Plaintiff resides. Plaintiffs may seek to add named Plaintiffs from these respective states so as to continue to assert these claims in a third consolidated amended complaint.

///

///

///


///

1 Defendants' motion to dismiss is denied in all other respects as provided herein. Plaintiffs'
2 third consolidated amended complaint shall be filed by **March 23, 2015**.

3 This order disposes of Docket No. 304.

4
5 IT IS SO ORDERED.

6
7 Dated: January 21, 2015

8 
9 EDWARD M. CHEN
10 United States District Judge
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28